unitar
United Nations Institute for Training and Research

Georgia Tech
Enterprise Innovation Institute

EXECUTIVE CYBERSECURITY TRAINING PROGRAMME

A capacity-building initiative for executives, senior managers and decision-makers.

Launching April 2026

01. Context

Cybersecurity is an increasingly important priority for organisations across both the public and private sectors. As digital systems become more central to operations, the number and complexity of cyber incidents have escalated dramatically. Cyberattacks in 2024 continue to affect key sectors such as manufacturing, transport and logiwhastics, telecom, and energy, with transport infrastructure, including airports and ports, emerging as a particularly frequent target for both state and criminal actors. A single incident at a major airport or port can cascade across global supply chains and travel networks, with consequences extending well beyond the organisation directly affected.

At the same time, a significant global cybersecurity talent gap persists, with over 3.4 million unfilled positions[1], alongside recurring challenges such as limited management support, insufficient trained personnel, and weak coordination across institutions. These gaps highlight the need to strengthen leadership awareness and capacity,which this programme aims to address by enabling more effective governance and support for cybersecurity efforts.

The **Executive Cybersecurity Training Programme,** offered by the United Nations Institute for Training and Research (UNITAR) and the Georgia Institute of Technology Enterprise Innovation Institute (EI2), aims to address this need by offering a customised programme designed to support executives and decision-makers in building a practical understanding of cybersecurity governance, risk management, and organisational resilience. It focuses on enabling leaders to make informed decisions, allocate resources appropriately, and strengthen the overall cybersecurity posture of their organisations.

A special emphasis is placed on cybersecurity at airports, ports, and critical transport infrastructure. Airports represent a uniquely complex cybersecurity environment: they combine IT systems (passenger management, ticketing, retail) with operational technology (OT) controlling runways, air bridges, baggage handling, and air traffic coordination. A successful cyberattack at a major hub can ground flights, disrupt cargo flows, compromise passenger safety systems, and trigger cascading effects across the entire aviation network.

Ports face structurally similar challenges, a cyber incident at a major port can halt cargo handling, block vessel movements, and send disruption rippling across international supply chains. Both environments share critical vulnerabilities: ageing OT systems not designed with cybersecurity in mind, a large and diverse ecosystem of third-party operators and

service providers, and senior leadership that is often better versed in operational logistics than in cyber risk governance.

The programme draws directly on Georgia Tech's deep expertise across both airport and port cybersecurity, including partnerships with U.S. federal agencies and extensive executive training delivered in over 40 countries, to provide transport infrastructure executives and senior managers with the tools to govern cybersecurity risk effectively.

02. Rationale

Cyber incidents do not typically arise from a lack of technology alone. They are often influenced by gaps in how cyber risk is understood and addressed at the leadership level. When decision-makers are not fully equipped to assess risks, interpret frameworks, or communicate the value of investment, organisations may face challenges in building effective resilience. Senior leaders without a baseline understanding of cybersecurity may find it more difficult to define risk appetite, guide the development of cybersecurity programmes, or support a culture that prioritises long-term resilience.

The business case remains strong. In 2024, the average cost of a data breach reached USD 4.88 million (IBM). Ransomware incidents continue to affect operations across sectors, including critical infrastructure. In July 2024, a faulty software update caused widespread disruption to Windows systems, with Delta Air Lines reporting approximately USD 380 million

in losses linked to over 7,000 cancelled flights. In parallel, supply chain attacks are increasingly targeting trusted third-party relationships, making cybersecurity maturity an important factor in securing and maintaining business partnerships.

Alongside operational considerations, regulatory and reputational expectations are also evolving. Customers, civil aviation and airport and port authorities, and supply chain partners increasingly seek evidence of cybersecurity maturity when awarding contracts or extending partnerships. Organisations that are unable to demonstrate a structured approach to cybersecurity may face limitations in accessing certain markets or opportunities.

This programme addresses three key needs:

1. **Enhancing awareness** of the business relevance of cybersecurity at senior organisational levels.
2. **Supporting executive-level understanding** of cybersecurity frameworks, governance approaches, and operational considerations, without requiring technical expertise.
3. **Offering practical and structured guidance** to help organisations initiate or strengthen cybersecurity programmes in line with their risk profile and industry context.

04. Programme Overview & Structure

The **Executive Cybersecurity Training Programme** is a 20-hour, non-technical capacity-building initiative designed for executives, senior managers, department heads, and organisational decision-makers. The programme is structured around three progressive learning sections and is designed for flexible delivery, with online content and bi-weekly online sessions.

Learning Modules

I. Core Concepts

- Why hacking attempts succeed, and how organisations create vulnerability
- Cyber risk, risk appetite, and organisational decision-making frameworks
- Definitions of cybersecurity and relevant compliance requirements
- Regulatory frameworks, legal obligations, and industry standards

- Return on investment in cybersecurity programmes
- Becoming a supplier of choice through strong cyber posture

II. Programme Initiation

- Matching cybersecurity requirements to organisational and sectoral contexts, including airports, ports, and logistics hubs
- Cyber assessments: internal/external, informal/accredited
- Introduction to Zero Trust Framework
- Basic cyber hygiene using NIST CSF and NIST 800-53
- Advanced cyber concepts: resiliency, response, and recovery
- Roadmaps, system security plans, Plans of Action & Milestones (PoA&Ms), and KPIs

III. Programme Maturity

- Policies and procedures: administrative, technical, and physical controls
- Employee training, insider threat awareness, and culture change
- Monitoring, intelligence gathering, and risk management
- Incident response planning and crisis communication
- Building and staffing a cyber team
- Tabletop exercises for crisis simulation

04. Expected Outcomes

Participants completing the Executive Cybersecurity Training Programme will:

- **Understand Threats:** Grasp core cyber threats and the business case for sustained cybersecurity investment.
- **Assess Readiness:** Evaluate organisational cyber posture and identify priority gaps and vulnerabilities.
- **Launch a Programme:** Initiate or refine a structured cybersecurity programme aligned with risk and industry requirements.
- **Apply Frameworks:** Make informed decisions using NIST, Zero Trust, and other recognised international standards.
- **Strengthen Governance:** Build internal culture, controls, and operational practices related to cybersecurity.

- **Gain Competitive Edge:** Enhance organisational credibility, resilience, and confidence of partners and clients.
- **Certification:** All participants receive a Georgia Tech / UNITAR Digital Certificate of Completion upon finishing the programme. Physical certificates are available upon request.

05. About the Partners

United Nations Institute for Training and Research (UNITAR)

UNITAR is the dedicated training arm of the United Nations system. Its mandate is to strengthen individual and institutional capacity through high-quality learning solutions, supporting global decision-making and sustainable development. UNITAR delivers capacity development primarily to developing countries, with special attention to Least Developed Countries (LDCs), Small Island Developing States (SIDS), and other vulnerable groups. Beyond its development mandate, UNITAR has an established track record of delivering executive-level training to government officials, international organisations, and private sector leaders worldwide, including in cybersecurity, transport, and critical infrastructure governance.

Georgia Institute of Technology, Enterprise Innovation Institute (EI2)

Georgia Tech is recognised as the top U.S. public university for cybersecurity and ranks among the five leading engineering schools worldwide. Its Enterprise Innovation Institute (EI2) represents the largest and most comprehensive university-based programme in the United States for business and industry support, technology commercialisation, and economic development. EI2 provides services to startups, corporations, the public sector, institutions, and students. Its work enhances competitiveness, converts innovative ideas into viable enterprises, and contributes positively to the global economy.

Georgia Tech's cybersecurity capabilities include:

- **Institute for Information Security & Privacy (IISP):** A leading university-based cybersecurity research institute
- **NSA-designated Center of Academic Excellence in Cyber Defense**
- Dedicated programmes in cybersecurity workforce development

- Expertise in **NIST Cybersecurity Framework** adoption, Zero Trust architecture, and NIST 800-53 implementation
- Established **public-private partnerships** with the U.S. Department of Defense, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Homeland Security (DHS)
- Executive cybersecurity training delivered in over **40 countries** through EI2 Global

05. Contact

To contact us, please reach out to transport@unitar.org.

[i] https://www.secureworld.io/industry-news/isc2-cybersecurity-industry-workforce-shortage