



# HudsonCyber

Managing Cyber Risk



Global



Innovative



Award-winning

## PORTLOGIX™

In today's hyper-connected business environment, ports and terminal operators are increasingly under cyber-attack.

Circumventing security protocols, cyber threat actors frequently gain unauthorized access to commercial data and networked IT/OT assets and systems, compromising data integrity and laying the groundwork for operational disruption. Such compromises can result in supply chain disruption, financial fraud and loss, first- and third-party liability exposure, regulatory fines, environmental damage, and even physical injury.

Port and terminal leaders are forced to contend with these dynamic, wide-ranging threats and related challenges, including the need to understand the cyber risks affecting their organizations, determine their impacts, and make informed decisions about how to most effectively and sustainably allocate finite resources to achieve any degree of cyber resilience.

PortLogix™ solves these challenges.

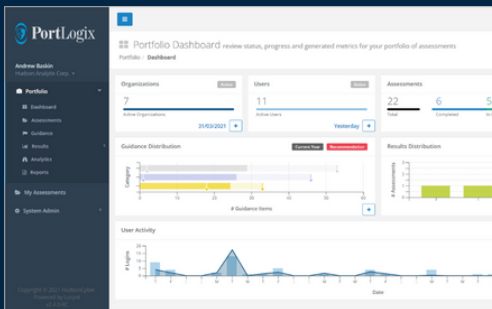
### PORTLOGIX™ EMPOWERS PORT-INDUSTRY STAKEHOLDERS TO:

- ✓ **Assess** cybersecurity capabilities across the entire organization
- ✓ **Identify** recommendations for mitigating identified gaps
- ✓ **Prioritize** investment planning and risk transfer decisions
- ✓ **Align** resources – people, processes, tools, and funding
- ✓ **Benchmark** cybersecurity capabilities against baselines and industry peers
- ✓ **Drive** cross-functional collaboration and continuous improvement
- ✓ **Govern** cybersecurity capabilities across port communities, information exchanges, and vendor base by implementing standardized, portfolio-driven Cyber-Supply Chain Risk management (C-SCRM)

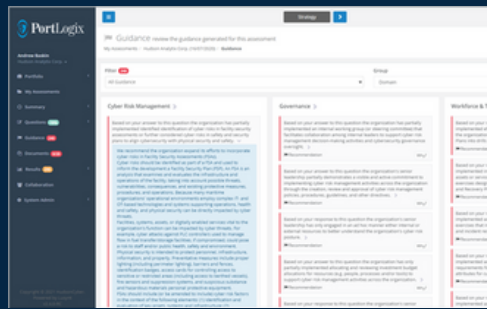


## KEY FEATURES AND BENEFITS

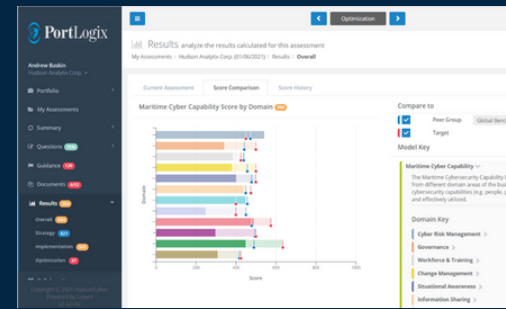
- **Rapidly establish** a cybersecurity program in as little as one day
- **Save money** by focusing resources on highest priority needs
- **Secure**, easy-to-use, 2FA enabled, cloud-based environment
- **Prioritized recommendations** are dynamically generated and available on demand
- **Real-time scoring** enables benchmarking and trend analysis
- **On-demand reports** available in multiple formats
- **Cultivate internal knowledgebase** with staff (instead of expensive consultants)
- **Multilingual** – available in English and Spanish



**Dashboard views** offer rapid access to key data sets with intuitive drill-down and filtering functions.



**Actionable recommendations** are prioritized and organized by functional domain. Filtering tools enable access to analyze critical information.



**Benchmarking** enables tracking progress against baseline capabilities and filtering to monitor performance against peers.

## APPLICABLE STANDARDS AND BEST PRACTICES

**PortLogix™ is based on a maturity-model methodology that helps ports and terminals align their cybersecurity program with:**

- NIST *Framework for Improving Critical Infrastructure Cybersecurity (V1.1)*
- NIST SP 800-82 (Rev. 2) *Guide to Industrial Control Systems Security*
- CIS *Critical Security Controls for Effective Cyber Defense (V7)*
- IMO *Guidelines on Maritime Cyber Risk Management (MSC-FAL.1-Circ.3-Rev.2)*
- ISO/IEC 27001:2013 RE: *Information Security Management Systems*
- ENISA *Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector*
- IAPH *Cybersecurity Guidelines for Ports and Port Facilities*
- OAS *Maritime Cybersecurity in the Western Hemisphere Guide*
- US DHS *Cybersecurity Capability Maturity Model (C2M2)*
- US Coast Guard *Maritime Cybersecurity Assessment and Annex Guide (MCAAG)* and NVIC No. 01-20, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security (MTSA) Regulated Facilities*
- US Customs-Trade Partnership Against Terrorism (C-TPAT) *Minimum Security Criteria: Cybersecurity*



HudsonCyber experts leverage extensive knowledge, skills, and expertise from both the cyber and physical security domains. We offer proven integrated cybersecurity strategies, advisory support, custom training, and tailored cyber threat intelligence to ports and port facilities of all sizes to assist them in understanding, managing, and mitigating their cyber risks.