Information Provided by Trident Group America, Inc

THE COMPLIANCE ILLUSION

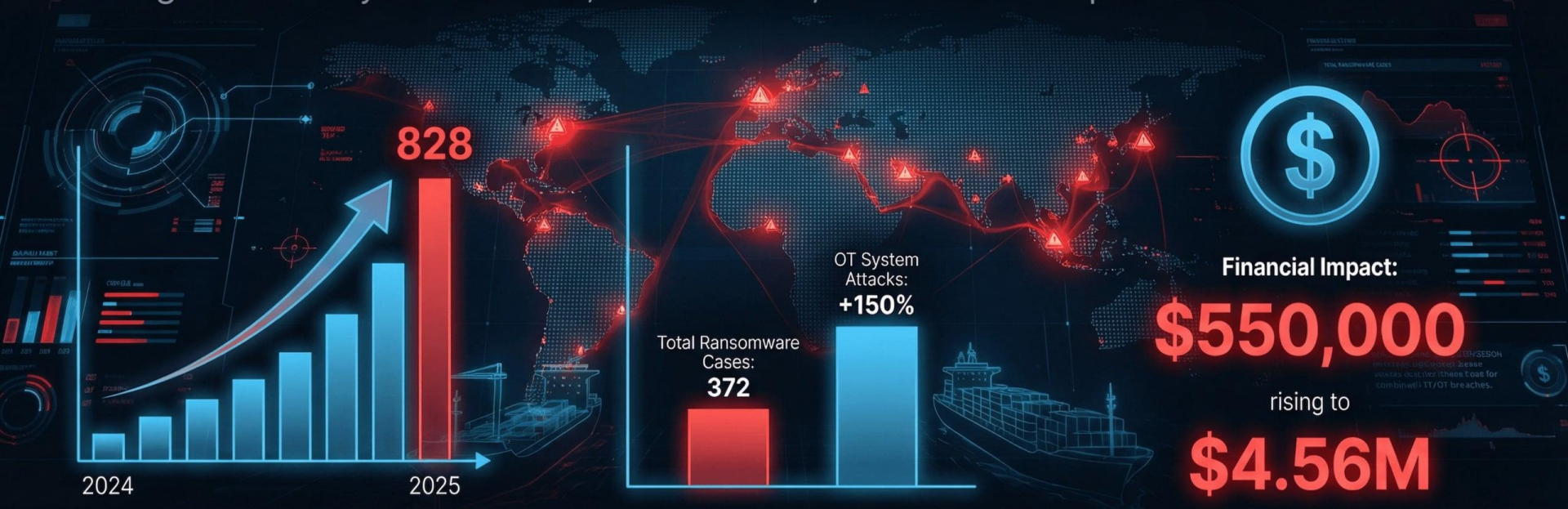
Why New Maritime Cyber Regulations Are Necessary but Not Sufficient.

Evolving threats and dynamic attack surfaces outpace static regulations. Compliance provides a baseline, but true resilience requires a proactive, continuous approach to cyber risk management beyond minimum standards.

Information Provided by Trident Group America, Inc

THE EXPLODING THREAT LANDSCAPE.

Rising Maritime Cyber Incidents, Ransomware, and Financial Impacts in 2025.



Surging Incidents: Maritime cyber incidents rose by 103% in 2025, reaching 828 documented cases.

Ransomware Surge: Cases more than doubled to 372, with OT system attacks increasing by 150%.

The average cost per incident exceeds $550,000, rising to $4.56M for combined IT/OT breaches.

Information Provided by Trident Group America, Inc

THE AI-DRIVEN ATTACK ERA

1. AUTONOMOUS THREATS

AI agents now perform up to 90% of an attack, from scanning to data theft.

2. ZERO-DAY DISCOVERY

AI identified 12 new zero-day vulnerabilities in OpenSSL in 2026.

3. RAPID EXPLOITATION

The window between discovery and exploitation has dropped to just 15 minutes.

THE USCG CYBERSECURITY RULE

Navigating the New Era of Maritime Cyber Regulations

KEY POINTS

- **MANDATORY FRAMEWORK:** The July 2025 rule mandates incident reporting and annual crew training.
- **PHASED ROLLOUT:** Cybersecurity Officers and formal plans are not required until July 2027.
- **COMPLIANCE GAP:** Reporting is a major step forward, but it is not a security control by itself.

JULY 2025
MANDATORY FRAMEWORK

2026

JULY 2027
PHASED ROLLOUT COMPLETE

Information Provided by Trident Group America, Inc

THE IACS E26 & E27 ARCHITECTURE

SYSTEM OF SYSTEMS

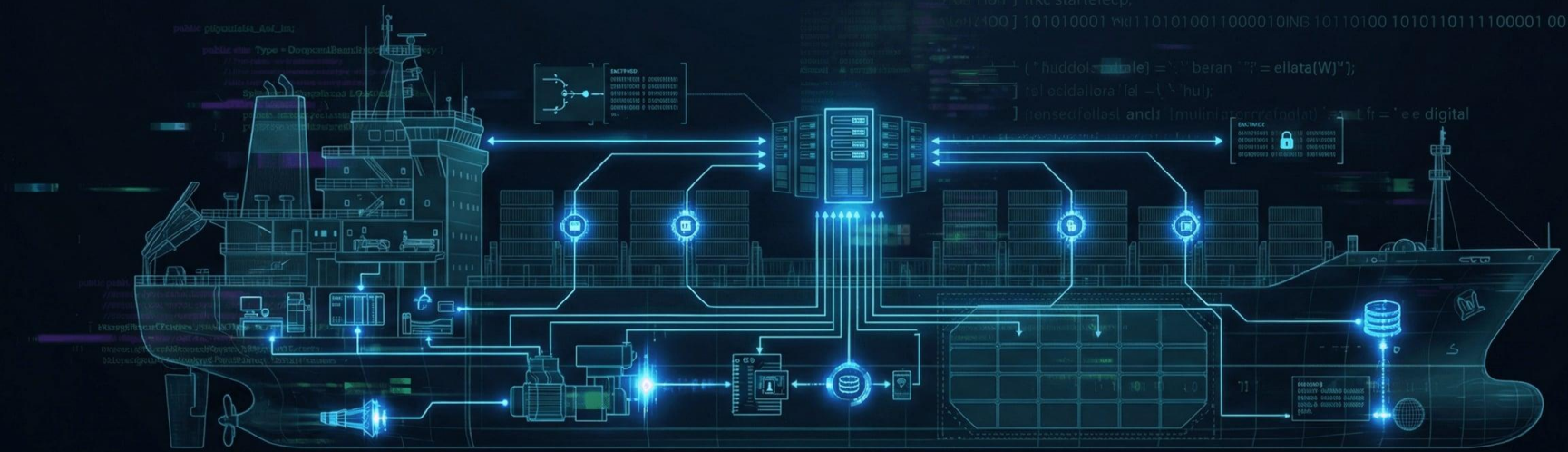
UR E26 requires network segmentation and strict IP exposure rules for new ships.

DEVICE-LEVEL SECURITY

UR E27 sets requirements for sensors, PLCs, and multi-factor authentication.

SCOPE LIMITATION

These standards are only mandatory for ships contracted after July 1, 2024.



Information Provided by Trident Group America, Inc

Information Provided by Trident Group America, Inc

THE LEGACY FLEET VULNERABILITY

Why New Maritime Cyber Regulations Are Necessary but Not Sufficient.

- **The 2024 Cutoff:** Most of the global commercial fleet consists of ships built before the new IACS standards.
- **Voluntary Compliance:** Existing vessels are only "strongly recommended" to adopt E26/E27, with no enforcement.
- **Older Systems:** Legacy ships run on systems designed for efficiency, leaving them exposed to modern threats.

Information Provided by Trident Group America, Inc

COMPLIANCE VS. REAL SECURITY.

Why New Maritime Cyber Regulations Are Necessary but Not Sufficient.

- **Paperwork Over Protection:** Organizations can pass audits while leaving OT systems open to uncontrolled access.
- **Basics Overlooked:** Common failures include unchanged default passwords and poor network separation.
- **Compliance Theater:** Drills and plans do not guarantee effectiveness without technical controls.

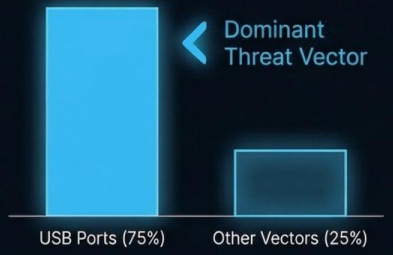
THE HUMAN ELEMENT & TRAINING

MANDATORY TRAINING

Annual cybersecurity training became mandatory in January 2026. This directive aims to ensure all personnel across the organization are equipped with the necessary knowledge to recognize and mitigate evolving digital threats.

THE USB THREAT

Uncontrolled USB ports caused 75% of maritime malware incidents in 2024. This high percentage underscores the critical risk associated with the use of external devices and the need for strict protocols.



OPERATIONAL REALITY

Training must move beyond modules to realistic, tested incident response. Simulating real-world scenarios with controlled, practical exercises is essential to build genuine readiness and effective decision-making under pressure.

Information Provided by Trident Group America, Inc

THE COST OF COMPLIANCE

Why Current Regulations Are Expensive and Potentially Misguided.

- **$1.2 Billion Investment:** The USCG rule is expected to cost the industry $1.2B over 10 years.
- **Process-Heavy Costs:** Most spending goes toward drills, exercises, and penetration testing.
- **Resource Allocation:** The danger lies in spending on documentation rather than technical resilience.

Information Provided by Trident Group America, Inc

GLOBAL REGULATORY CONVERGENCE

Multiple Regimes: Operators face a complex web of IMO, USCG, IACS, and EU NIS2 regulations.

NIS2 Penalties: The EU's directive imposes fines up to €10M or 2% of global annual revenue.

Unified Signal: The industry can no longer ignore cyber risk as a core operational safety issue.

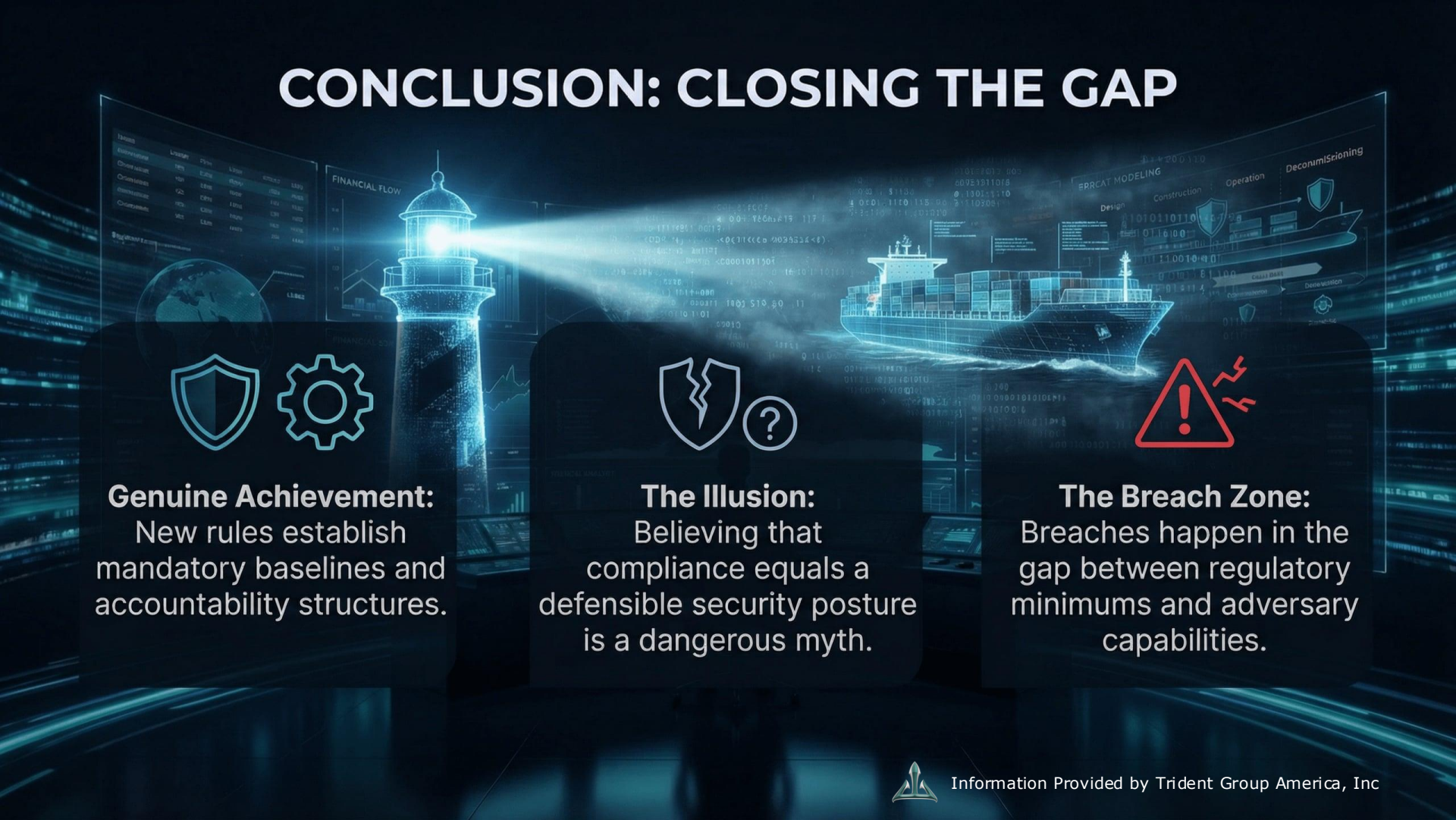
SHIFTING TO INTELLIGENCE-DRIVEN RESILIENCE

Beyond Minimums: Regulations are the floor, not the ceiling; security must be proactive.

Threat Modeling: Integrating security from the design stage through the vessel's entire lifecycle.

Resilience Focus: Shifting from just preventing incidents to anticipating and recovering from them.

CONCLUSION: CLOSING THE GAP



Genuine Achievement:
New rules establish mandatory baselines and accountability structures.

The Illusion:
Believing that compliance equals a defensible security posture is a dangerous myth.

The Breach Zone:
Breaches happen in the gap between regulatory minimums and adversary capabilities.

TRIDENT GROUP AMERICA

Leaders in Maritime & Cyber Security

- Specialized Maritime Cyber Red Cell
- Global Maritime Security Solutions
- Asset Protection (Sea, Air, Land)
- Professional Training & Security Operations

Information Provided by Trident Group America, Inc