Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about the U.S. and Indonesia tabletop exercise that was recently conducted and highlights the importance of continually exercising cyber incident response across your business environment.

Summary

From June 10-13, 2024, the U.S. and Indonesia conducted their inaugural port-focused cybersecurity tabletop exercise in Surabaya, Indonesia. The exercise was spearheaded by the U.S. Department of Homeland Security (DHS), with support from the U.S. State Department and various Indonesian government entities. The primary goal was to bolster the resilience of maritime critical infrastructure against cyber threats through simulated cyber incidents and ransomware attacks on port operations and ship-to-shore cranes.

Exercise Overview

Throughout the exercise the following objectives were set out and activities conducted:

- **Objectives:**
  - Stress Test Cyber Incident Response Plans: Assess the effectiveness of current response plans in handling major cyber incidents.
  - Enhance Collaboration: Foster stronger coordination between U.S. and Indonesian entities to secure the maritime domain from cyber threats.
  - Identify Gaps: Pinpoint areas for improvement in cyber resilience and incident response.

- **Activities:**
  - Simulation of Cyber Incidents: Participants engaged in realistic simulations of cyberattacks on port operations, including ransomware scenarios affecting ship-to-shore cranes and other critical systems.
  - Workshops and Discussions: Post-exercise workshops led by the U.S. Coast Guard covered best practices in maritime cyber incident prevention and response.

Key Outcomes

The exercise enabled the following outcomes:

- **Improved Incident Response**
  - The exercise provided a platform to evaluate and improve incident response strategies, allowing participants to test their preparedness and identify weaknesses in their current plans.

- **Increased Awareness of Cyber Risks**
  - Discussions and simulations raised awareness among stakeholders about the growing sophistication of cyber threats in the maritime environment, underscoring the need for a comprehensive approach that integrates coordination, capacity building, and information sharing.

- **Policy and Best Practice Sharing**
    - The U.S. Coast Guard's workshop facilitated the exchange of policies and best practices related to cyber incident management, providing valuable insights for Indonesian stakeholders on how to enhance their cybersecurity measures.

Significance and Future Directions

The exercise has allowed key stakeholders to roadmap the direction to be taken going forward in relation to strategic operational resilience decision making, including:

- **Addressing Vulnerabilities in Critical Infrastructure**
    - The exercise highlights the critical need to address vulnerabilities in critical infrastructure, particularly in light of concerns over Chinese-built cranes and broader cyber threats from state-backed actors like China's Volt Typhoon campaign.

- **Continued Investment in Cybersecurity**
    - Ongoing investments are crucial for strengthening cyber defenses and mitigating the risks posed by modern cyber threats.

- **Building Resilience Through Exercises**
    - Regular cybersecurity exercises and tabletop simulations are essential for building resilience, testing response capabilities, and forging partnerships that can effectively counter cyber threats.

Conclusion

The U.S.-Indonesia port-focused cybersecurity tabletop exercise marks a significant step toward enhancing the cyber resilience of critical infrastructure. By engaging in such exercises, organisations, regardless of their industry or size, can gain valuable insights into potential cyber vulnerabilities and strengthen their defenses against threats that could disrupt operations or cause financial loss. Through collaborative efforts, realistic simulations, and the sharing of best practices, the exercise has laid the groundwork for improved incident response, stronger bilateral ties, and a more secure maritime domain.

Participation in these exercises not only helps companies develop robust incident response strategies and cyber defenses but also promotes a culture of proactive risk management and preparedness. Future initiatives should continue to build on these successes, ensuring that both nations and their diverse industries are well-prepared to face the evolving landscape of cyber threats.

References

1. The Record: https://therecord.media/indonesia-port-maritime-cybersecurity-exercise-united-states

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team