Building a Cyber Security Culture in Maritime Industry

topics

- cyber security landscape
- cyber security development
- cyber level
- focus on culture – create the Cyber Business Leader
- cyber security culture effectiveness

cyber security impacts (2021)

- remote working
- covid-19 crisis exploitation
- ransomware/phishing challenges
- OT automations & data analysis (AI)
- real time monitoring & visibility
- insiders threats – new era // computerized seafarers
- regulations

Cyber Security Developments (2021)

- MFA/PAM – remote working
- security infrastructure hardening
- advanced threat protection for business functions
- cyber threat intelligence (Security Operation Centers)
- invest in CISO/Cyber security workforce
- invest in awareness (insiders threats)
- invest in processes (Regulations: TMSA3, IMO)

Cyber level - Question: Are we secure?

- cyber space is extended
- more cyber related processes have been added
- more technology has been implemented
- more training has been conducted

✓ **But, are we secure?**

Towards to cyber comfort

- Do you know how your employees feel with Cyber Security?
- Do they feel comfortable or not
- Are we ready to go from Cyber readiness to Cyber Comfort?

Cyber Business Leader

Focus was to:

- build interconnected digital environments that will secure the exchange of the data, meaning to create a secure Cyber Space

Focus should be to: create the **Cyber Business Leader**

- the person that will feel comfortable exchanging data in the Cyber Space, while will be a defender of our infrastructure

✓ Invest in Cyber Security Culture (CSC)

CSC Definition

Provided by Enisa:

- ✓ Cybersecurity Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies.

Goal is to:

- Create a cyber security mindset
- Foster security awareness and risk perception

CSC Factors

Factors that influence the CSC are:

1. External:
   - Regulations
   - Technological developments
   - Integration with 3rd parties

2. Internal:
   - Clear direction provided by Top Management – Translate needs to business metrics
   - Cyber Security Team /CISO
   - Employees: perception, academic background, nationality, age, personalities, behavior and beliefs

CSC – Internal Factors in Maritime

Focus on Internal Factors

Employees: academic background, nationality, age, personalities, behavior and understanding

Invest in Cyber Security Culture – Use of Holistic Approach that includes:

- Analysis of business processes – tailor made security policies / friendly to the end user
- Customized Training per department / role / process
- KPIS to measure the effectiveness of procedures / training & human behavior
- Cyber Security Culture Assessment

CSC – Internal Factors in Maritime

Analysis of Business processes:

- Create Roles & responsibilities per operation process
- Identify the cyber security perception of relevant employee
- Align business functions with Cyber Security Policies

✓Create **trust and comfort** on day to day business

CSC – Internal Factors in Maritime

Customized awareness training:

- Customized training per department
- Fill relevant gaps
- From learning to reacting

✓ Cyber Security human reaction on incidents should follow relevant process and use common sense

CSC – Internal Factors in Maritime

KPIS to measure the effectiveness of procedures / training & human behavior

- Create Cyber Security Campaigns and Drills (onshore & offshore)
- Measure the effectiveness of cyber security procedures
- Measure the effectiveness of Cyber Security Awareness
- Measure the Human behavior vs Compliance vs Culture
- Promote Cyber Security leadership
- Celebrate small wins

CSC – Internal Factors in Maritime

Cyber Security Culture Assessment

Assess:

- Cyber Security Policy & Procedures
- User's perceptions of the protection of information assets
- User's understanding on Cyber Security Policy
- User's need of awareness and training
- Cyber Security leader per department
- User's ability for change
- User's trust on working with organization's private data

Invest in humans

“At the end of the day we rely on human beings”

Thank you