Securing OT through People

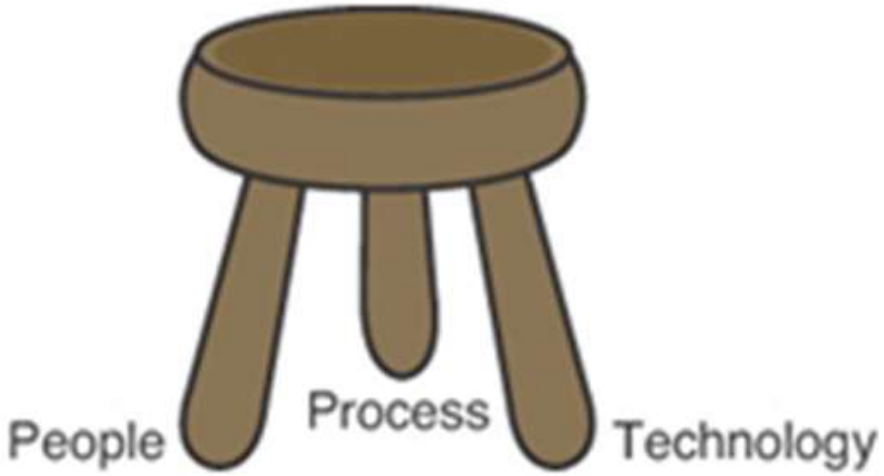
Grivas Kostas

Information Security Officer

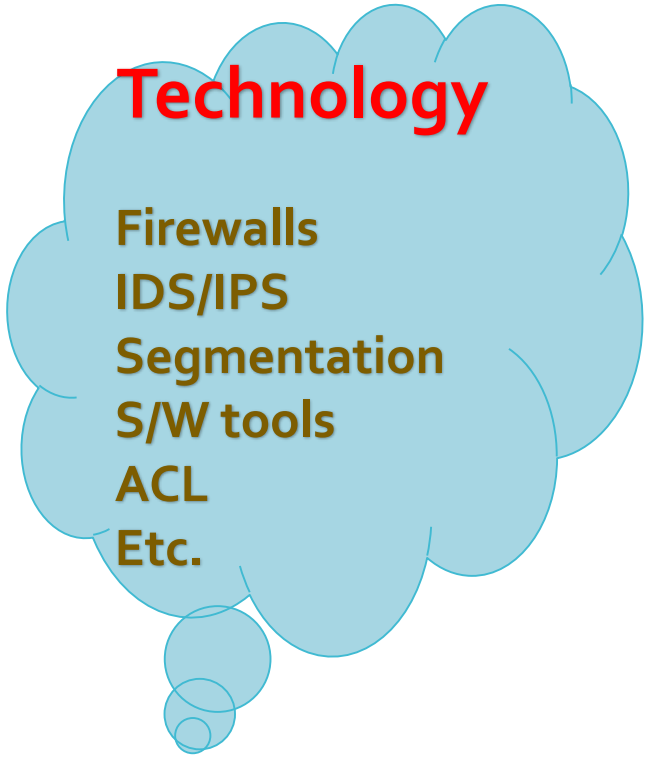
5th ShipIT Conference, Athens, September 26, 2019

Digital Systems Security Framework

OT Security



The Framework Surface



Scratching under the Surface

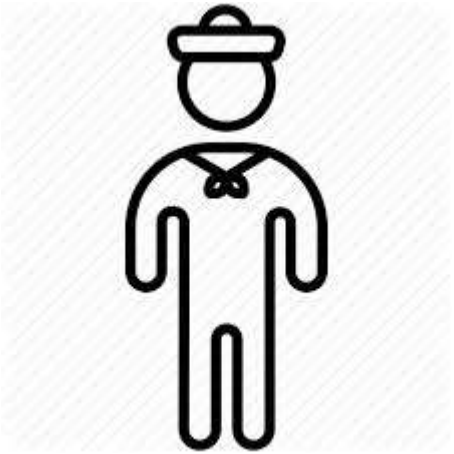
Cyber Incident root cause

Technology	**Properly designed, configured and maintained H/W or S/W, rarely lead to Cyber Incidents.**
Processes	**Well-developed and established processes, rarely lead to Cyber Incidents.**
People	**Negligence, ignorance, lack of knowledge, wrong decision, or just failure doing the basics are the usual reason.**

People

Management

Seafarers



IT Personnel

Employees

Suppliers

Management

Cyber Security is a Top – Down activity. Everything starts from the Management.

Requirements

- ***Senior Management must understand the General Strategy***
- ***Risk based analysis, at the higher level, with Risks & Impact***
- ***Departments' Managers to understand threats, in more details***
- ***Equipment and software installation in cooperation with IT/Security***
- ***Procedures & processes based on Operational & Security needs***

✓ ***It is vital that the Management embrace and support our strategy.***

Employees

The Employees involved in OT systems cluster.

- *Like Departments' Managers, they must understand threats, in more details*
- *Maintain and audit OT systems' use with a Cyber safe mindset.*
- *Develop procedures and processes to be Cyber security compliant.*
- *Have good knowledge of the Vessel Cyber Security Policy and guidelines.*
- *Be Cyber Security aware.*
- ***Become our valuable sponsors***

Seafarers

Probably one of the two MOST critical links of the OT systems defense chain.

- ***Must understand the Serious impact of an incident to the vessel's overall safety***
- ***Have good knowledge of the Vessel Cyber Security Policy and guidelines.***
- ***Their interaction with OT the systems makes them potential threat actors and defenders.***
- ***No matter the countermeasures and protection you have applied, just like on the shore side, a significant percentage of cyber events occur due to users' behavior.***
- ***Make them the Human Firewall O/B***

When People are "missing"

= **Cyber safe**

= **Booby Trap**

Suppliers, makers & other 3rd parties

Probably the second MOST critical link of the OT systems defense chain

- ***Makers***
  - *Re-define their R&D to consider the threat landscape*
  - *Educate/train their personnel and retain awareness*
- ***Service Companies***
  - *Educate/train their personnel and engineers and retain awareness*
  - *Adopt Cyber security mentality*
- ***Authorities & other Bodies***
  - *Accelerate their pace and lead the Cyber Security race*

Digital Technology and threats are moving much faster than they anticipate

IT Personnel

The last but not the least of the "People Universe"

- *Tech savvies but not necessarily Cyber Aware*
- *Usually provide the "last mile" of the OT systems connection to the real world. It is important to understand the impact*
- *Are they truly familiar with the systems and technology they use? When was their last course?*
- *Like Seafarers, they are our Human Firewall. They are our advantage*
- *Educate them, don't just train them.*

Conclusion

Ultimately, the objective should be a Sailor/Person who understands cyber hygiene and proper use of the network as a primary on-the-job tool, just as well as any Soldier knows his or her rifle.

Sailors/Persons go to sea aboard complex ships with integrated networked systems that run everything from Hull, Cargo, Mechanical, and Electrical (HM&E) systems.

The computer is our rifle, why shouldn't we learn how to use it more safely and effectively?

"Center for International Maritime Cybersecurity"

Conclusion