TANKEROperator

6th Tanker Operator Hamburg conference - October 19, 2017
People, performance and technology

Maintaining staff passion in shipping - continuing our improvement in safety
October 19th, 2017

Lack of cybersecurity from marine approved systems

Presented by: Jose Milhazes

Stolt-Nielsen - Global Manager
Stolt Tankers B.V - Business Process Manger SNSO
j.milhazes@stolt.com
Mobile: +31 6 21507845

http://www.stolt-nielsen.com

Agenda:

1. Cyber-Security Introduction
2. True cost of Cyber-Attacks
3. No Business is Safe
4. Unsafe Onboard Systems
5. Conclusions - Next

Cyber-Security Introduction

In today's business globalization all sizes organizations face the treats of falling victim of cyber-attack or IT outage that can cause serious damage to it's infrastructure and ability to do day to day operations

Despite all effort an improvements in cyber-security techniques , criminals continue to develop sophisticated ways to disrupt systems and steal, destroy or encrypt our data.

The need to prepare for cyber-attack is more important than ever, and need to be a combine effort from customers to suppliers, from small to high organizations.

True cost of Cyber-Attacks

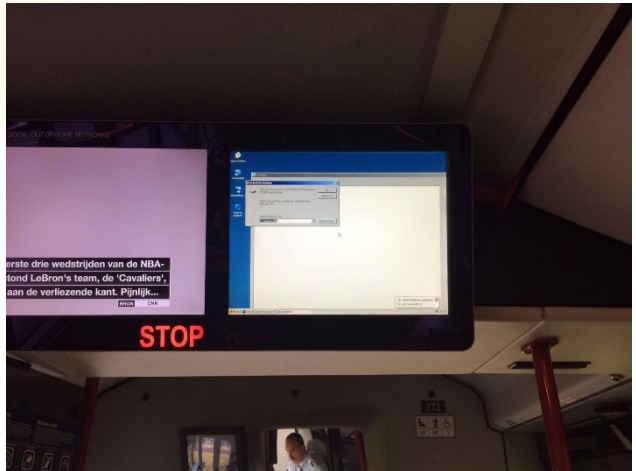
According to Cisco 2017 Annual Cybersecurity report (1)

- More than one third of the organizations that experienced a cyber breach in 2016 reported a loss of customers, business opportunities and revenue.

The 2017 SonicWall Annual Threat report (2)

- In 2015 the number of cyber-attacks reported were 3.8 Million
- In 2016 the number reach 638 Million

In average it takes more than 31 days to a company recover from a cyber attack, but as more small business is getting attack with low potential to recover this is been increasing over the years.

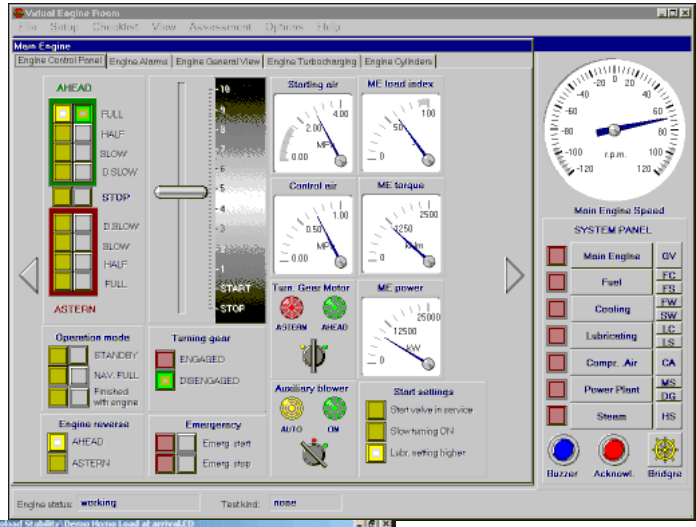


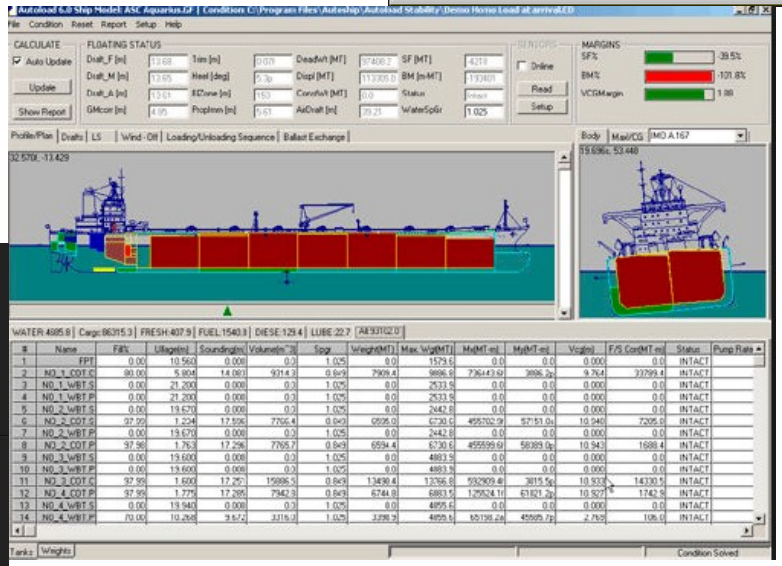
No Business is Safe

- Hackers attacked the backbone of the NHS, tapping into computers, telephones system, MRI scanners, blood-storage refrigerators and others equipment's (May, 2017).
- Doctors, surgeons had to use their mobile phones to communicate, X-ray's and other vital patients information were share by DVD's.
- Lesson's learn show us that it is easy to forget when a portfolio of internet devices to enable internet needed to be updated for security.
- With the internet of things (IoT) expected to consist of millions of new connected devices in the future – this issue will become more critical.
- Investing large sums of money in to cyber-security is not a pre-requisite for success (as shown by a number of recent high profile cyber-attacks against known corporations)
- Not just large organizations are target.
- When attacks occur crucial services are compromised, your reputation will be effected near your customers.

Unsafe Onboard Systems

- Antivirus, and OS security patch's are critical to OT security.
- M/E control, navigation and Cargo systems are deployed and expected not to be updated.
- Most of those systems are NOW running under Windows XP or lower versions OS.
- None of those PC's are running any type of antivirus.
- AND they are CERTIFY by authorities, to be keep as deployed (20y)





Conclusions - Next

As no business or organization is totally immune from the dangers of a cyber-attack it's vital that crisis management plans are in place to minimize impact and ensure a return to business-as–usual practice as quickly, safe and operational as possible.

Approach your existing suppliers and address your concerns on cyber-security and business continuity

Thank you

Questions?

Jose Milhazes
j.milhazes@stolt.com

1-”Cisco 2017 Annual Cybersecurity Report Chief Security Officers Reveal True Cost of Breaches And The ActionsThat Organizations Are Talking” Cisco Systems, Inc N.p., n.d. web 20 Jnune 2017

2-https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/