THE AMERICAN CLUB

CYBER SECURITY: A P&I PERSPECTIVE

DOROTHEA IOANNOU

Chief Commercial Officer

Shipowners Claims Bureau Inc., Managers,

American Steamship Owners Mutual

Protection and Indemnity Association

NAMEPA & AMCHAM - SEMINAR "*TRADING IN US WATERS: PRIORITIES AND SOLUTIONS*"

P&I Insurance

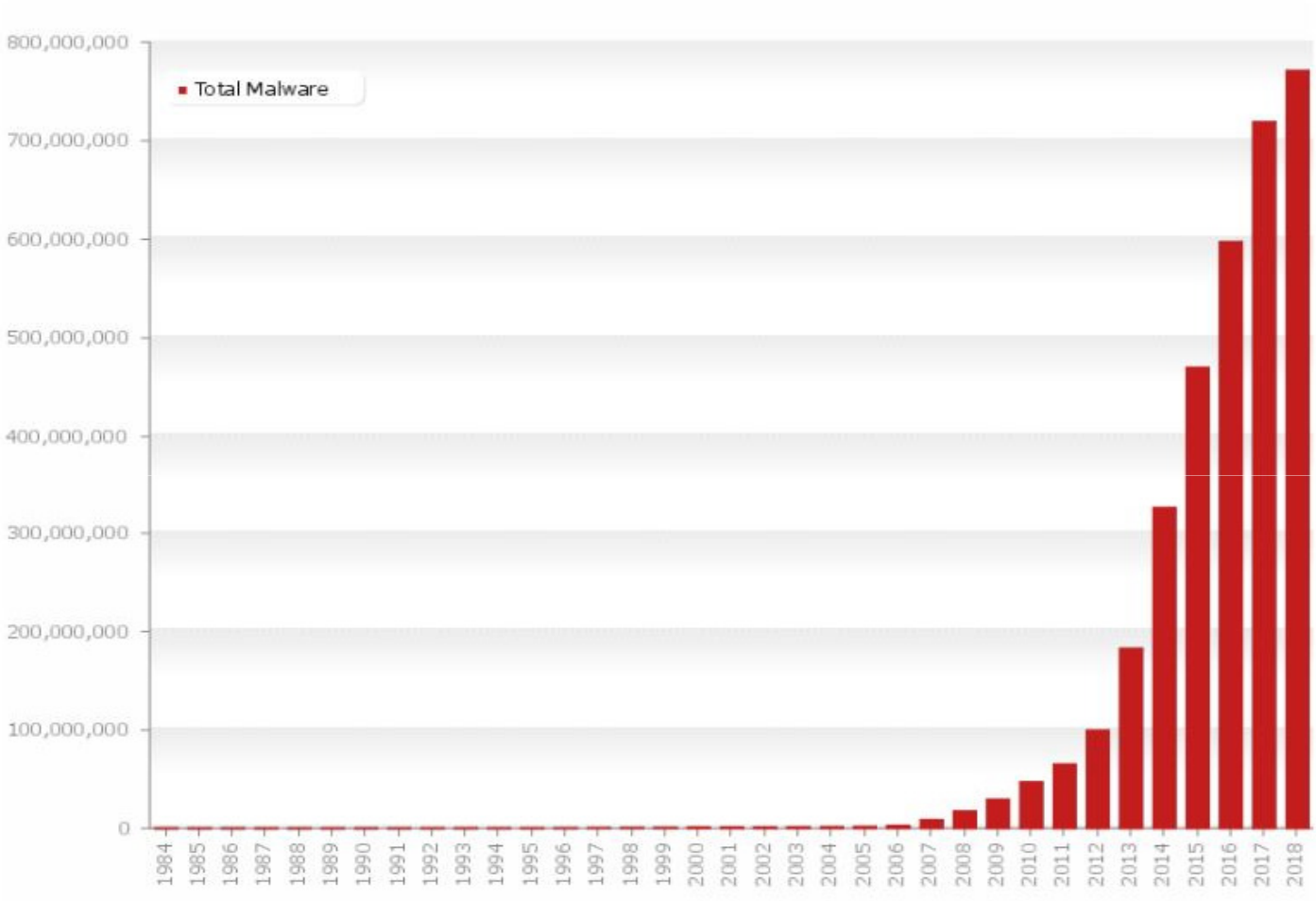
- Third Party Liability
- Types of liabilities covered expressed in Rules
- The Unique part of P&I : created BY shipowners FOR shipowners

Ships Then & Now.
Tomorrow ?

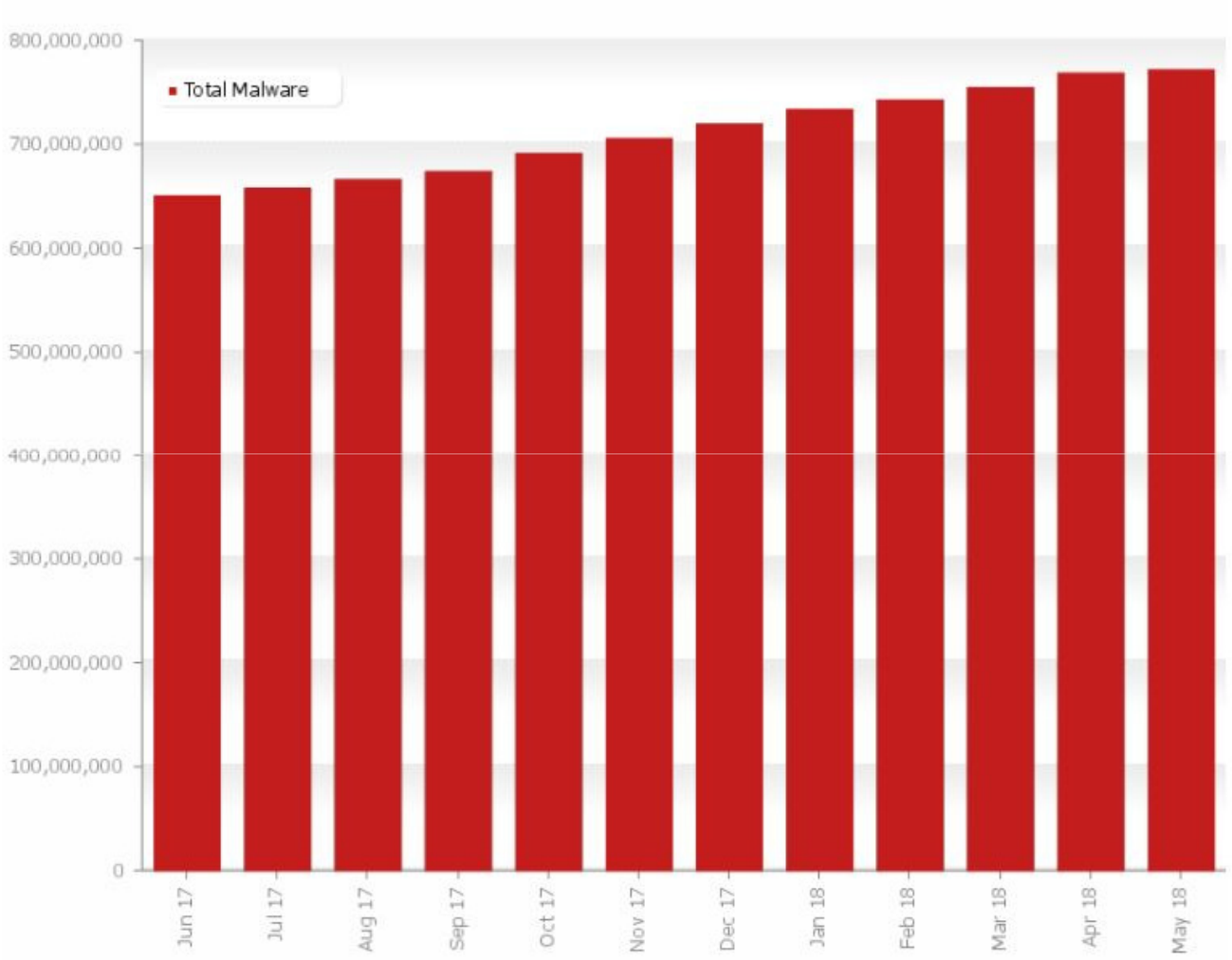
P&I & Cyber Threat

- P&I – most loss caused by human error
- P&I Clubs place great emphasis in all loss prevention through knowledge and awareness training
- Human error is a significant factor contributing to Cyber attack losses
- Cybercrime finds gaps created by human disregard and lack of awareness/training
- Common element is Human Factor

Malware Growth



Malware Growth (last 12 months)



Human Factor and Malware

- Egan, G. (2018). Connecting the Dots: The Human Factor and the Cost of Cybercrime.

Seafarer Awareness

- 47% of seafarers said that they had sailed on a vessel that had been the target of a cyber-attack.

- Only 15% of seafarers had received any form of cyber security training. The majority of training currently provided to seafarers is by crewing and manning agencies before the seafarer leaves on his/her next contract.

Seafarer Awareness

- Only 33% of seafarers said the company they last worked for had a policy to regularly change passwords on board.
- Only 18% of seafarers said the company they last worked for had a policy to change default equipment passwords on board.
- Only 20% cited cyber security training.

Crew Connectivity Survey Report

2018

Mitigating & Preventing

- Building awareness through training and education
- American P&I club: internal cyber security training and certification for ALL staff

Mitigating & Preventing

THE AMERICAN CLUB
100 YEARS OF SERVICE 1917 2017

Mitigating & Preventing

- Awareness training part of your operational culture

- Learn how to spot RED FLAGS

How does P&I insurance respond to cyber attack losses?

Scenario 1

- Unauthorized access into an agent's email system
- Impersonation of the agent
- Funds directed to impersonator's bank account
- Fraud
- Own economic loss falls outside standard P&I cover
- FD&D
- Learn to spot the red flags

Scenario 2 (a)

- Malware is installed by seafarers' mistake (e.g. infected USB stick) interferes with its navigation systems and leads to collision, injury, death etc.
- P&I would respond in the normal course
- Training & policies = lead to *prevention*

Scenario 2 (b)

- Compromised monitoring system (known terrorist acknowledges responsibility)
- Falls into war & terrorism exclusion
- Training and policies mitigate risk

Scenario 3

- A virus is planted by seafarers' mistake and causes engine malfunction.
- Delay costs
- Outside of standard P&I cover

Guidelines and Initiatives

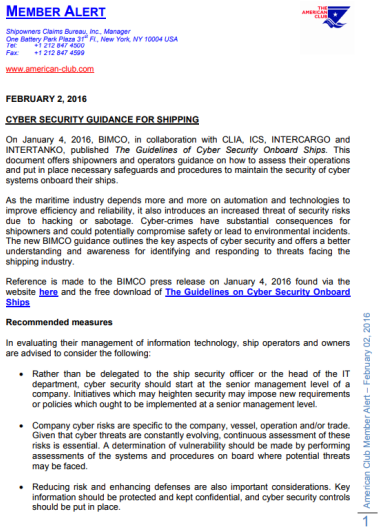
- IMO
- USCG
- BIMCO
- ICS Alerts
- ICS Advisors
- ICS-CERT Monitor Newsletter

- Visit: https://www.us-cert.gov/security-publications

American P&I Club

- Promoted by The American P & I Club to Members, with reminders of recommended measures
- Member Alert- American Club Cyber Security Guidance issued 2/2016:

http://www.american-club.com/files/files/MA_020216_Cyber_Security_Guidance_for_Shipping.pdf



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

FEBRUARY 2, 2016

CYBER SECURITY GUIDANCE FOR SHIPPING

On January 4, 2016, BIMCO, in collaboration with CLIA, ICS, INTERCARGO and INTERTANKO, published *The Guidelines of Cyber Security Onboard Ships*. This document offers shipowners and operators guidance on how to assess their operations and put in place necessary safeguards and procedures to maintain the security of cyber systems onboard their ships.

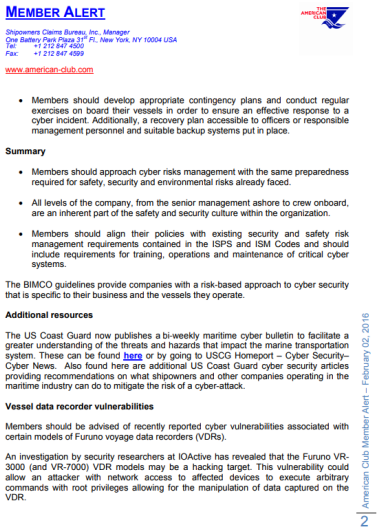
As the maritime industry depends more and more on automation and technologies to improve efficiency and reliability, it also introduces an increased threat of security risks due to hacking or sabotage. Cyber-crimes have substantial consequences for shipowners and could potentially compromise safety or lead to environmental incidents. The new BIMCO guidance outlines the key aspects of cyber security and offers a better understanding and awareness for identifying and responding to threats facing the shipping industry.

Reference is made to the BIMCO press release on January 4, 2016 found via the website **here** and the free download of **The Guidelines on Cyber Security Onboard Ships**

Recommended measures

In evaluating their management of information technology, ship operators and owners are advised to consider the following:

- Rather than be delegated to the ship security officer or the head of the IT department, cyber security should start at the senior management level of a company. Initiatives which may heighten security may impose new requirements or policies which ought to be implemented at a senior management level.
- Company cyber risks are specific to the company, vessel, operation and/or trade. Given that cyber threats are constantly evolving, continuous assessment of these risks is essential. A determination of vulnerability should be made by performing assessments of the systems and procedures on board where potential threats may be faced.
- Reducing risk and enhancing defenses are also important considerations. Key information should be protected and kept confidential, and cyber security controls should be put in place.



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

- Members should develop appropriate contingency plans and conduct regular exercises on board their vessels in order to ensure an effective response to a cyber incident. Additionally, a recovery plan accessible to officers or responsible management personnel and suitable backup systems put in place.

Summary

- Members should approach cyber risks management with the same preparedness required for safety, security and environmental risks already faced.
- All levels of the company, from the senior management ashore to crew onboard, are an inherent part of the safety and security culture within the organization.
- Members should align their policies with existing security and safety risk management requirements contained in the ISPS and ISM Codes and should include requirements for training, operations and maintenance of critical cyber systems.

The BIMCO guidelines provide companies with a risk-based approach to cyber security that is specific to their business and the vessels they operate.

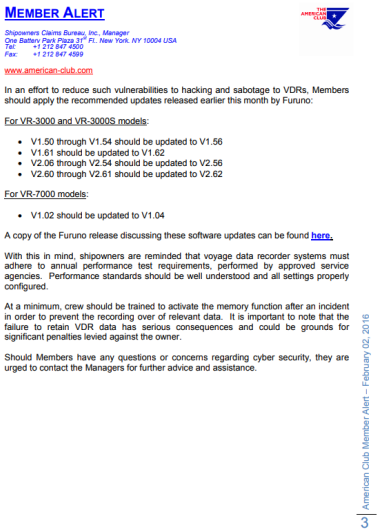
Additional resources

The US Coast Guard now publishes a bi-weekly maritime cyber bulletin to facilitate a greater understanding of the threats and hazards that impact the marine transportation system. These can be found **here** or by going to USCG Homeport – Cyber Security– Cyber News. Also found here are additional US Coast Guard cyber security articles providing recommendations on what shipowners and other companies operating in the maritime industry can do to mitigate the risk of a cyber-attack.

Vessel data recorder vulnerabilities

Members should be advised of recently reported cyber vulnerabilities associated with certain models of Furuno voyage data recorders (VDRs).

An investigation by security researchers at IOActive has revealed that the Furuno VR-3000 (and VR-7000) VDR models may be a hacking target. This vulnerability could allow an attacker with network access to affected devices to execute arbitrary commands with root privileges allowing for the manipulation of data captured on the VDR.



MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

In an effort to reduce such vulnerabilities to hacking and sabotage to VDRs, Members should apply the recommended updates released earlier this month by Furuno:

For VR-3000 and VR-3000S models:

- V1.50 through V1.54 should be updated to V1.56
- V1.61 should be updated to V1.62
- V2.06 through V2.54 should be updated to V2.56
- V2.60 through V2.61 should be updated to V2.62

For VR-7000 models:

- V1.02 should be updated to V1.04

A copy of the Furuno release discussing these software updates can be found **here.**

With this in mind, shipowners are reminded that voyage data recorder systems must adhere to annual performance test requirements, performed by approved service agencies. Performance standards should be well understood and all settings properly configured.

At a minimum, crew should be trained to activate the memory function after an incident in order to prevent the recording over of relevant data. It is important to note that the failure to retain VDR data has serious consequences and could be grounds for significant penalties levied against the owner.

Should Members have any questions or concerns regarding cyber security, they are urged to contact the Managers for further advice and assistance.

Cyber Risk & Insurance

- Evaluate your operations – your insurance needs
- Refer to industry & regulatory guidelines
- No cyber exclusions for P&I but it does not cover every consequence of every scenario
- Consult experts – fill your insurance gaps
- Training and education will promote a stronger cyber culture

Questions?

Thank you!

Acknowledgements

- Egan, G. (2018). Connecting the Dots: The Human Factor and the Cost of Cybercrime. Retrieved from https://www.wombatsecurity.com/blog/phishing-social-engineering-the-human-factor-and-the-cost-of-cybercrime
- Milkovich, D. (2018). 12 Alarming Cyber Security Facts and Stats | Cybint. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/
- Cyber Crime | Statista. (2018). Retrieved from https://www.statista.com/markets/424/topic/1065/cyber-crime/
- AV-TEST – The Independent IT-Security Institute. (2018). Retrieved from https://www.av-test.org/en/statistics/malware/
- 2018 Cybercrime Statistics: A closer look at the "Web of Profit". (2018). Retrieved from https://www.thesslstore.com/blog/2018-cybercrime-statistics/
- Futurenautics Ltd. 2018 | The Shard (2018). Retrieved from https://www.osm.no/PageFiles/4520/Crew_Connectivity_2018_Survey_Report.pdf
- Picture slide 3 : https://www.google.gr/search?q=ship+in+the+past&rlz=1C1NHXL_elGR775GR775&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjDl9qHkrLbAhUGDZoKHefxDRsQ_AUICigB&biw=2133&bih=1082#imgrc=jpL9JPTnIiOkcM:
- Picture slide: 12 https://www.google.gr/search?biw=2133&bih=1027&tbm=isch&sa=1&ei=hRIRW73kF8aQmwWNvLTICg&q=cyber+terrorist&oq=cyber+ter&gs_l=img.1.1.0i19k1l10.809582.812068.0.814905.9.9.0.0.0.0.136.940.0j8.8.0....0...1c.1.64.img..1.8.939...0j0i67k1j0i10k1.0.9UT_caP_z7A#imgdii=JLz5sEE9jzsSCM:&imgrc=CwQI81671-uLpM:
- Picture slide 10: https://www.google.gr/search?q=account+fraud&rlz=1C1NHXL_elGR775GR775&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi7sPWpnbLbAhUPLVAKHYYgCPQQ_AUICigB&biw=2133&bih=1027#imgrc=2enJxL3tMuKeIM:
- Picture slide 13: https://www.google.gr/search?rlz=1C1NHXL_elGR775GR775&biw=2133&bih=1027&tbm=isch&sa=1&ei=4RwRW_KYNMnQwALGwqGwCg&q=delay&oq=delay&gs_l=img.3..0l6j0i30k1l4.32043.33549.0.34477.5.5.0.0.0.0.166.608.0j5.5.0....0...1c.1.64.img..0.5.607...0i67k1.0.FobHj9m-ccE#imgrc=OklN8Lq5vn1yfM: