



International Port Security Program



Port Facility Cyber Security

Seminar Introduction



Overview



The Cyber Security Seminar is not a “certification” program. Participation in and completion of the seminar in no way provides any recognized certification credentials.



Overview



Methods and templates presented throughout this course are derived from U.S. and other international best practices and are not considered a comprehensive list.



Introductions



- Name
- Agency
- Port Security Responsibilities
- Goals for the Seminar





Does It Matter To Me?



- Do you own, operate or occupy a port or port facility that has electronic or computer based systems?
- If the port systems were to fail, malfunction or were misused would this result in economic, operational, physical or reputational loss or damage, or disrupt operations?





Does It Matter To Me?



- Do you own an information asset that includes information about your strategy and/or commercial operations, the operation of your port or port facility, including any port systems?
- If this information asset were compromised could this result in economic, operational, physical or reputational loss or damage?





Does It Matter To Me?



Yes

No



Seminar Introduction



- What is Cyber Security?





Seminar Introduction



Cyber security is not just about preventing hackers gaining access to systems and information. It also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of cyber assets.





Seminar Introduction



To achieve this, consideration needs to be given to protecting systems from physical attack and designing port systems and supporting processes to be resilient.





Seminar Introduction



Personnel security aspects are also important, as the insider threat from staff or contractors who decide to behave in a malicious way cannot be ignored.





Seminar Introduction



- What negative consequences do organizations face as a result of poor Cyber Security?





Seminar Introduction



- Failure to address security risks could lead to:
 - serious injury or fatality;
 - disruption or damage to port systems;
 - loss of use of buildings;
 - impact upon business operations;





Seminar Introduction



- Failure to address security risks could lead to (cont):
 - reputational damage;
 - loss of revenue; and
 - financial penalties or litigation.





Seminar Introduction





Works Cited



Code of Practice Cyber Security for Ports and Port Systems

Authors: Hugh Boyes, Roy Isbell and
Alexandra Luck

Published by: Institution of Engineering and
Technology, London, United Kingdom

First published 2016



U. S. COAST GUARD