Port Facility Cyber Security

What is Cyber Security?

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.

What is Cyber Security?

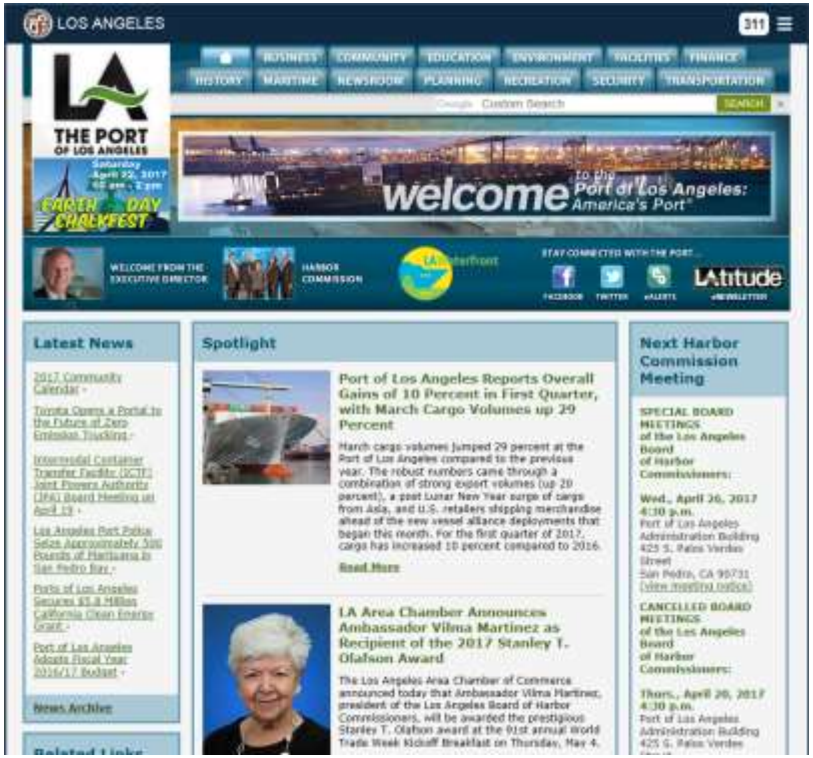
Cyber security can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the **cyber environment** and **organization and user's assets**."

What is Cyber Security?

Within this definition, 'cyber environment' comprises the interconnected networks of both information and cyber physical systems that use electronic, computer-based and wireless systems, including information, services and social and business functions that exist only in cyberspace.

What is Cyber Security?

PayPal™



Latest News

2017 Community Calendar ›

Toyota Opens a Portal to the Future of Zero Emission Trucking ›

Intermodal Container Transfer Facility (ICTF) Joint Powers Authority (JPA) Board Meeting on April 19 ›

Los Angeles Port Police Seize Approximately 500 Pounds of Marijuana in San Pedro Bay ›

Ports of Los Angeles Secures $5.8 Million California Clean Energy Grant ›

Port of Los Angeles Adopts Fiscal Year 2016/17 Budget ›

News Archive

Related Links

Spotlight

Port of Los Angeles Reports Overall Gains of 10 Percent in First Quarter, with March Cargo Volumes up 29 Percent

March cargo volumes jumped 29 percent at the Port of Los Angeles compared to the previous year. The robust numbers came through a combination of strong export volumes (up 20 percent), a post Lunar New Year surge of cargo from Asia, and U.S. retailers shipping merchandise ahead of the new vessel alliance deployments that began this month. For the first quarter of 2017, cargo has increased 10 percent compared to 2016.

Read More

LA Area Chamber Announces Ambassador Vilma Martinez as Recipient of the 2017 Stanley T. Olafson Award

The Los Angeles Area Chamber of Commerce announced today that Ambassador Vilma Martinez, president of the Los Angeles Board of Harbor Commissioners, will be awarded the prestigious Stanley T. Olafson award at the 91st annual World Trade Week Kickoff Breakfast on Thursday, May 4.

Next Harbor Commission Meeting

SPECIAL BOARD MEETINGS
of the Los Angeles Board
of Harbor Commissioners:

Wed., April 26, 2017
4:30 p.m.
Port of Los Angeles
Administration Building
425 S. Palos Verdes Street
San Pedro, CA 90731
(view meeting notice)

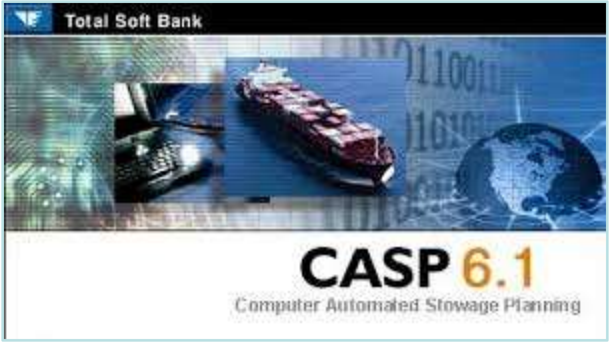
CANCELLED BOARD MEETINGS
of the Los Angeles Board
of Harbor Commissioners:

Thurs., April 20, 2017
4:30 p.m.
Port of Los Angeles
Administration Building
425 S. Palos Verdes

What is Cyber Security?

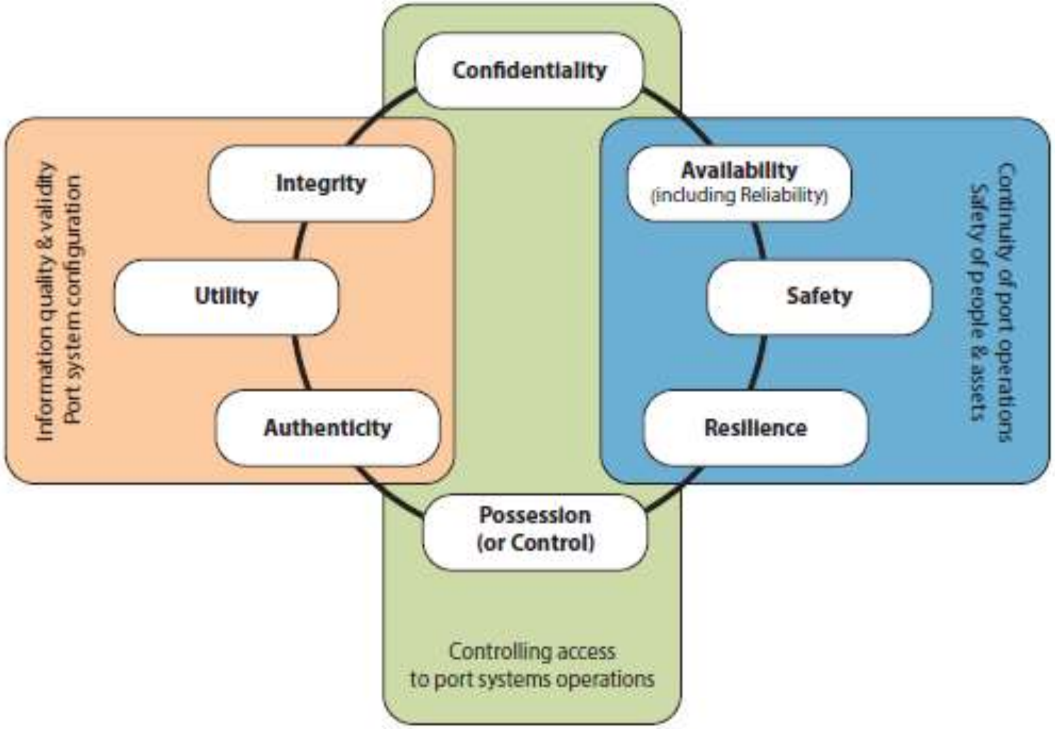
The organization and user's assets' includes connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed and/or stored data and information in the cyber environment.

What is Cyber Security?



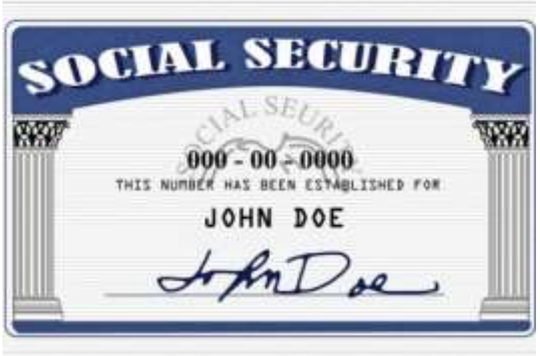
What is Cyber Security?

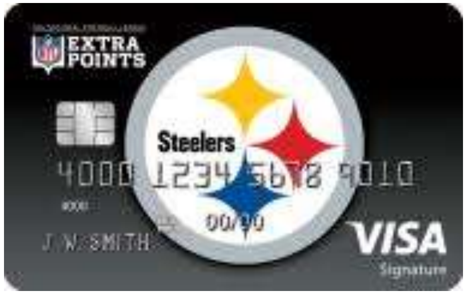
Cyber security strives to attain and maintain eight general security objectives.


Confidentiality
Integrity
Utility
Authenticity
Availability
(including Reliability)
Safety
Resilience
Possession
(or Control)
Information quality & validity
Port system configuration
Continuity of port operations
Safety of people & assets
Controlling access
to port systems operations

What is Cyber Security?

Confidentiality – the control of access and prevention of unauthorized access to port data, which might be sensitive in isolation or in aggregate.





What is Cyber Security?

Integrity – maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorized changes to them.

What is Cyber Security?

Authenticity – ensuring that inputs to, and outputs from, port systems, the state of the systems and any associated processes and port data, are genuine and have not been tampered with or modified.

What is Cyber Security?

Availability (including reliability) – ensuring that the asset information, systems, and associated processes are consistently accessible and usable in an appropriate and timely fashion.

What is Cyber Security?

Availability (cont) – A loss of availability could occur through the failure of a system component, such as a disk crash, or from a malicious act such as a denial of service attack that prevents the use of a system connected to the Internet.

What is Cyber Security?

Upgrading Windows

Your PC will restart several times. Sit back and relax.

12%

Copying files 4%

Installing features and drivers

Configuring settings

Utility – ensuring that asset information and systems remain usable and useful across the lifecycle of the port asset.

What is Cyber Security?

Utility (cont) – An example of loss of utility would be a situation where a port system has been changed or upgraded and the file format of historic data is no longer intelligible to the system. There has been no loss of availability but the data is unusable.

What is Cyber Security?

Safety – the design, implementation, operation and maintenance of port systems and related processes so as to prevent the creation of harmful states that may lead to injury or loss of life, or unintentional physical or environmental damage.

What is Cyber Security?

Safety (cont) – A safety issue could arise through malware causing a failure to display or communicate port systems alarm states. For example, the failure of a motion or proximity detector or other sensors could result in damage to property or loss of life.

What is Cyber Security?

Resilience – the ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events. The design, implementation, operation and maintenance of port systems and associated processes should be such that cascade failures are avoided.

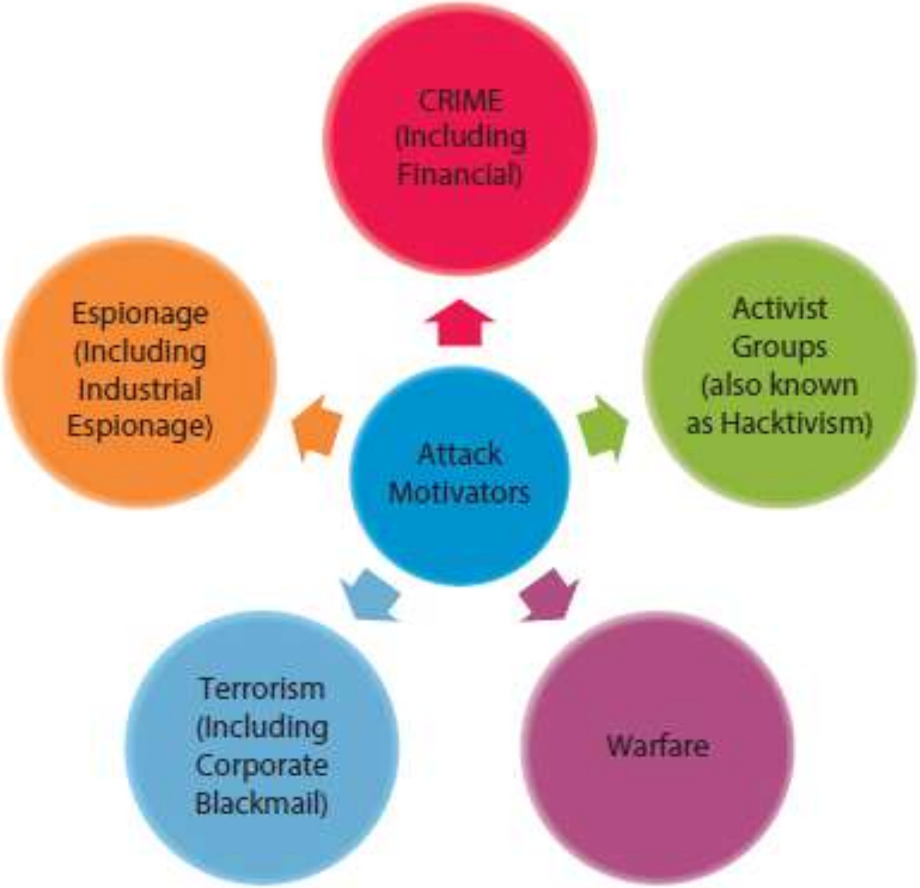
What is Cyber Security?

Resilience (cont) – In the event that either a system or associated process suffers disruption, impairment or an outage occurs, it should be possible to recover a normal operating state, or acceptable business continuity state, in a timely manner.

Motivations

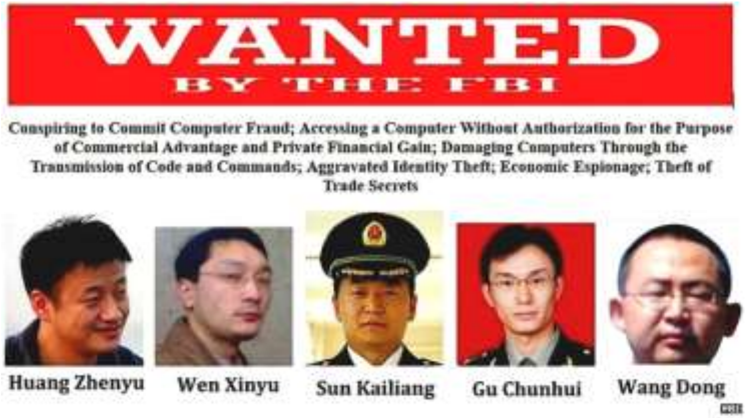
What motivates groups/individuals to conduct cyber attacks?

Motivations


CRIME (Including Financial)
Espionage (Including Industrial Espionage)
Attack Motivators
Activist Groups (also known as Hacktivism)
Terrorism (Including Corporate Blackmail)
Warfare

Motivations

Espionage – seeking unauthorized access to sensitive information (intellectual property, commercial information, corporate strategies, personal data, pattern of life) and disruption for state or commercial purposes.



WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu Wen Xinyu Sun Kailiang Gu Chunhui Wang Dong

Motivations

Activist Groups (also known as 'hacktivism') – seeking publicity or creating pressure on behalf of a specific objective or cause, for example, to prevent the handling of specific cargos or to disrupt construction of a new port facility.

Motivations

Criminal – largely driven by financial gain, this can include criminal damage, theft of cargo, smuggling of goods and people, and attempts to evade taxes and excise duties.

Motivations

Terrorism – use of the port to instill fear and cause physical and economic disruption.

Motivations

Warfare – conflict between nation states, where the aim is disruption of transport systems/infrastructure to deny operational use or disable specific port facilities, such as bulk terminals.

Threat Actor Groups

Why motivates groups/individuals to conduct cyber attacks?

Threat Actor Groups

Individual: The severity and sophistication of the threat will be determined by the individual's capabilities.

Threat Actor Groups

A negligent, careless or ignorant employee or contractor fails to follow acceptable use or other security policies, or through error or omission compromises system security.

Threat Actor Groups

“Friendly" individuals who are not seeking to harm systems or data, but may access the systems without the permission or knowledge of the owner and may cause accidental damage. The motivation of such agents is generally to investigate weaknesses and vulnerabilities in systems.

Threat Actor Groups

A disaffected employee or contractor with limited IT skills – motivations will vary; the intent may be to steal or leak sensitive information, to sabotage or disrupt port occupancy or operations, etc. The amount of damage they can inflict will depend on their role, system access rights and the efficacy of cyber security measures related to the port systems and data.

Threat Actor Groups

Disaffected employee or contractor with significant IT skills, including system administrators – these individuals can do significant damage, particularly if they have wide-ranging systems access with administrative privileges.

Threat Actor Groups

They may have sufficient knowledge and ability to bypass controls and protective measures, and may be adept at removing evidence of their activities, for example, deleting or modifying entries in system logs.

Threat Actor Groups

Script kiddies – individual hackers with limited knowledge who use techniques and tools devised and developed by other people. The ready availability of hacking and denial-of-service tools on the Internet means that the level of technical understanding required to launch an attack has been significantly reduced.

Threat Actor Groups

Cyber Vandals – such individuals can be very knowledgeable and may develop or further expand their own tools. Their motives are neither financial nor ideological – they carry out hacks or develop malware because they can and want to show what they can do. They may, for example, deface a website to demonstrate their ability.

Threat Actor Groups

Lone Wolf – an individual outside of the organization possessing advanced technical knowledge. Such an individual may be adept at removing evidence of their activities, for example, deleting or modifying entries in system logs. They may also have sufficient knowledge and ability to bypass controls and protective measures.

Threat Actor Groups

Activist Groups: Often referred to as activists, these groups comprise ideologically motivated individuals that may form dynamic groups or sub-groups.

Threat Actor Groups

Activist Groups (cont): Their actions are effectively online protests, which may have the aim of disrupting systems or acquiring confidential or sensitive information for publication or dissemination so as to embarrass their target(s).

Threat Actor Groups

Cyber Criminals: These are sophisticated criminal groups perpetrating a wide range of illegal IT-enabled crime. The motivation is to profit from illegal activities, and their focus has mainly been on fraud, thefts from accounts and theft of intellectual property.

Threat Actor Groups

Cyber Criminals (cont): In respect of ports, cyber criminals may seek to intercept or access information related to cargo shipments or to security arrangements as a precursor to criminal activities or a physical attack on these premises.

Threat Actor Groups

Terrorists: Terrorists are becoming increasingly IT aware, and already make extensive use of the Internet to distribute propaganda and for communications purposes. Well-funded groups could take advantage of the service offered by cyber criminals, seek support from a nation state or encourage internal members to adopt these methods of attack.

Threat Actor Groups

Nation States: It is acknowledged that some nation states are actively involved in cyber-attacks on a wide range of organizations to acquire state secrets or sensitive commercial information and intellectual property.

Questions

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