November 4, 2021

Maritime/ Port Cybersecurity

Marine Technology Society

Daniel E. Turissini

Chair, Maritime Cyber Security and Infrastructure Committee

turissd@mac.com

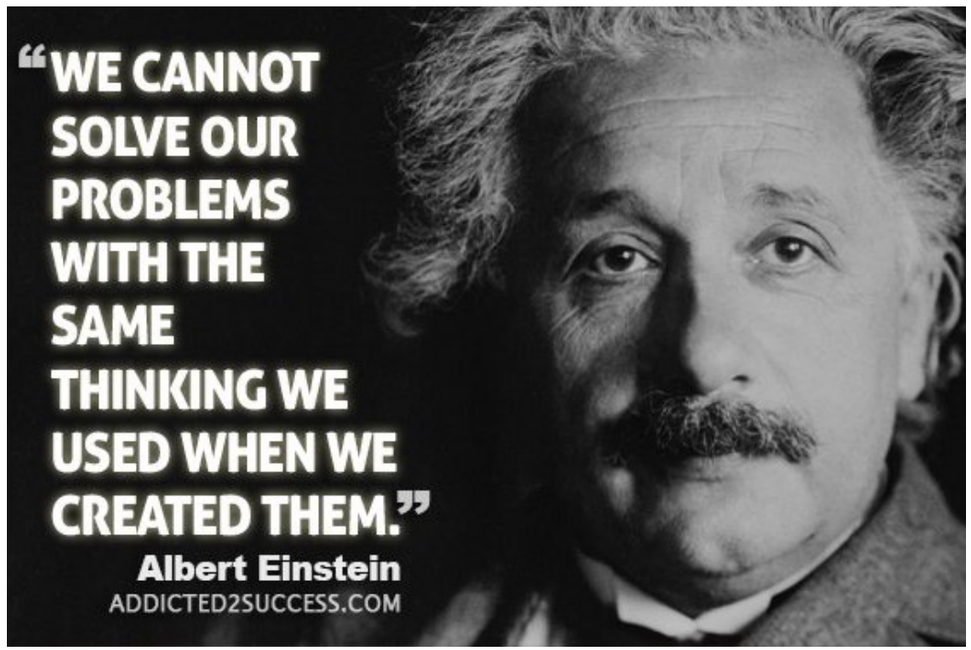
Introduction

- Instructor: Daniel E. Turissini (“Dan”)
  - 35+ years Security, Information Security, Information Assurance, Cyber Security
  - Certified as a Cyber Instructor and Compliance Assessor
  - Chair, Marine Technology Society Maritime Cyber Security and Infrastructure Committee
  - Board Member, AFCEA International
  - Vice Chair, AFCEA Homeland Security Committee
  - Serial Entrepreneur: CTO, CISO, CEO (Software, Hardware and Managed Services)
  - BS, United States Merchant Marine Academy: Marine Engineering & Nautical Science
  - Masters Engineering Administration, Systems Engineering George Washington University
  - My wife & I of 40 years have 3 grown sons, 3-year old granddaughter & 3-month old grandson
  - Enjoy Boating/ Sailing, Fishing, Golf & relaxing on the beach
- LOOKING FORWARD TO AN INTERACTIVE PRESENTATION

Cybersecurity must be driven from the top

marine technology SOCIETY
Opportunity runs deep™

- Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report
- The average cost was USD 1.07 million higher in breaches where remote work was a factor in causing the breach
- The most common initial attack vector, compromised credentials



[Source: IBM Cost of a Data Breach Report 2021]

Cyber Security as a cost avoidance investment

marine technology SOCIETY
Opportunity runs deep™

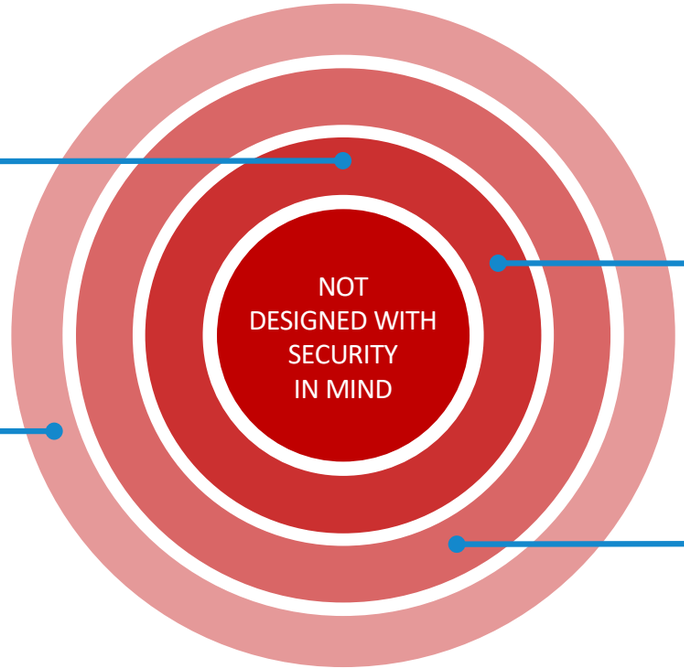
- Provide adequate protection of end entity authentication credentials that meet mandated government **data & privacy protection requirements**, while **ensuring timely sharing** of information to its stakeholders
- Enhance **accountability** of the sensitive information by providing strong mutual authentication & non-repudiation of interactions with Cyber services by leveraging existing & compliant technologies
- Provide a **path to compliance** with emerging requirements (not limited to US Federal Data Security and GDPR compliance requirements) & avoid unnecessary costs that may arise from system silos & stove piping
- Enhance existing capability by providing timely & relevant information sharing, communicating alerts and **enhancing educational services**

An opportunity to capitalize on USG investment

marine technology SOCIETY
Opportunity runs deep™

Updates not signed & verifiable (security flaws; new code)

Vulnerabilities of software security solutions (not using hardware-based protection)

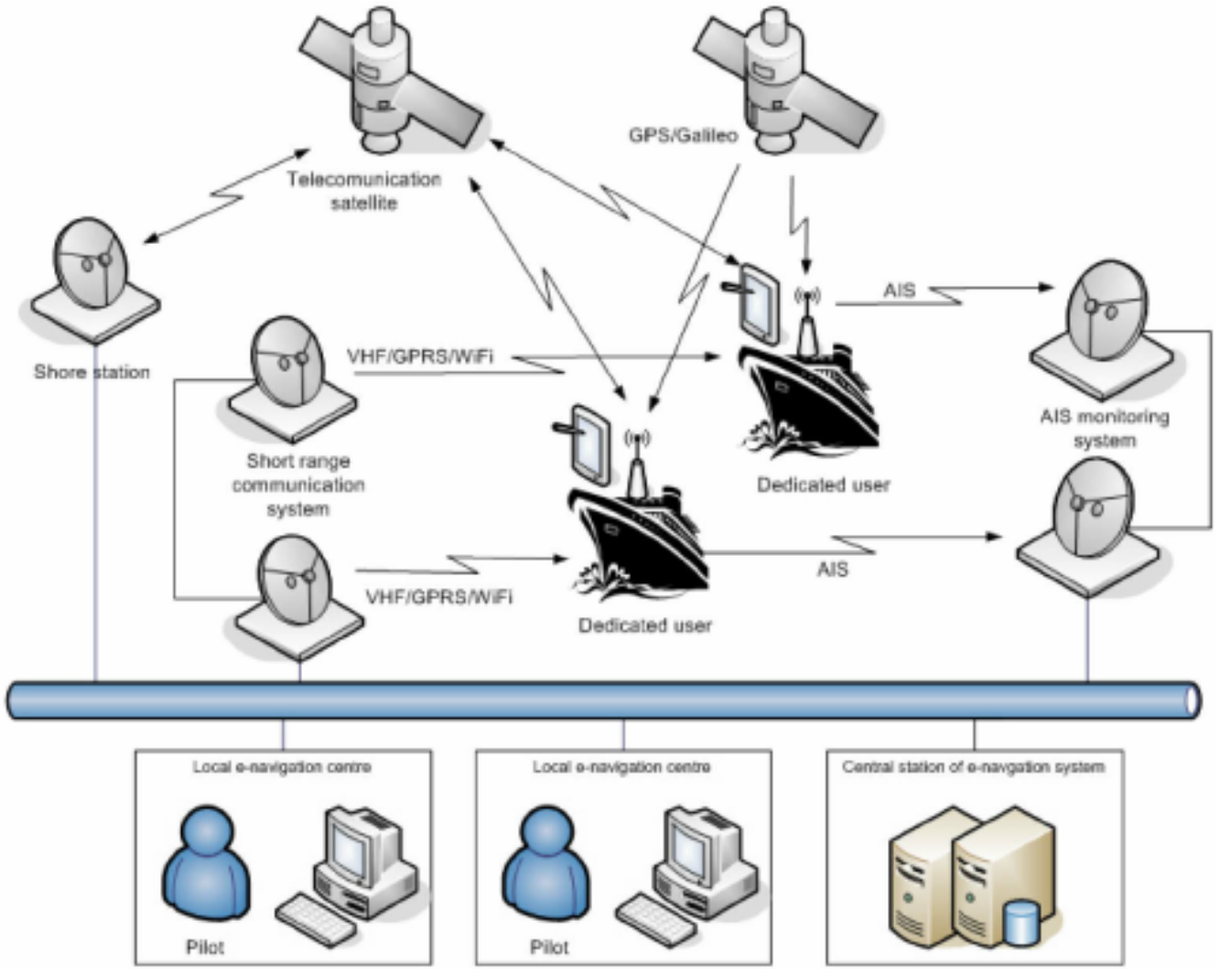


60% of devices do not use encryption when downloading software updates

Device ID & serial numbers exposed in software

As the industry moves to more autonomy and Artificial Intelligence, addressing these design flaws is essential to Safety of Life at Sea & Ashore

The Goal is Authoritative Communications



- Avoid unauthorized disclosure
- Tools:
  - Encryption
  - Access Control
  - Physical Security

- Avoid unauthorized changes
- Tools:
  - Digital Signature
  - Backup/ Archiving
  - Checksum
  - Data Correcting code

- Accessible & usable in a timely fashion
- Tools:
  - Physical Protections
  - Redundancy

Data We Can Trust

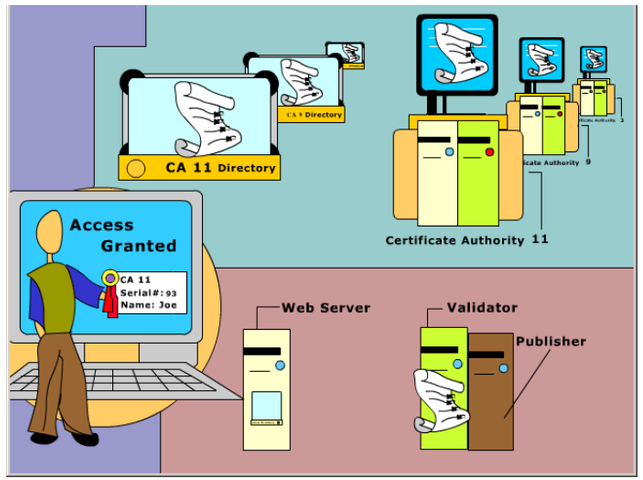
Cyber Security based on who & what, not where!

marine technology SOCIETY
Opportunity runs deep™

A Systems Eng. approach to achieve …

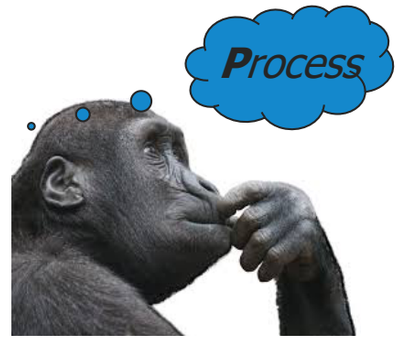
***N**on-repudiation*

***A**uthenticity*



***P**rivilege & **A**uthorization*

… at each information state

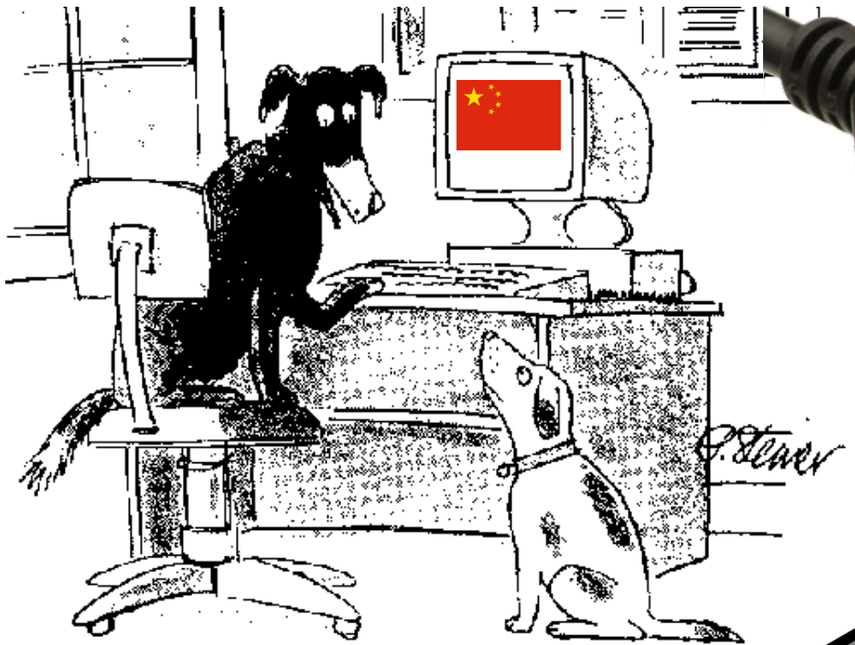


People, devices, servers , objects, IoT, code ….

Still a Common Root Vulnerability

marine technology SOCIETY
Opportunity runs deep™

We still offer little or no mechanism to confidently know the difference between legitimate & illegitimate parties/ entities transacting - while agreeing that they are the largest vulnerability.



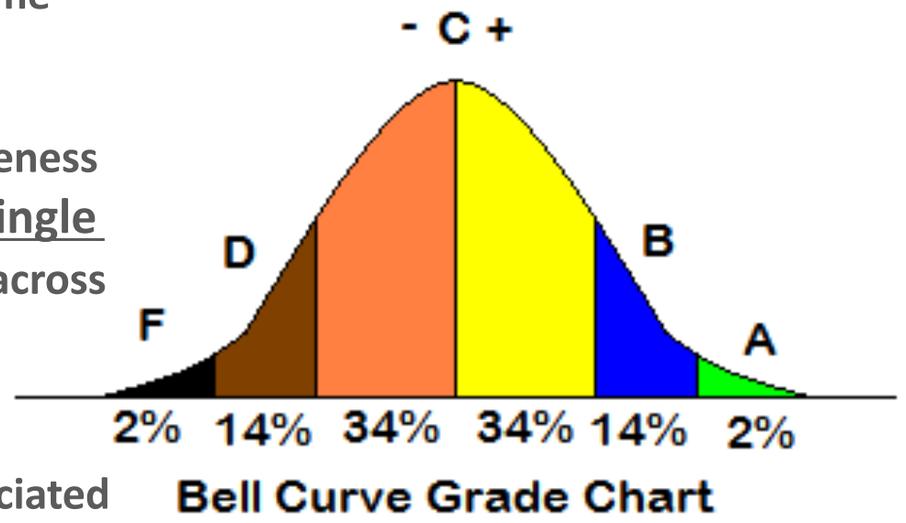
Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20) ... mic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title ... S. Code

Phishing, Ransomware & other similar attacks can be mitigated with strong & simple relying party identity validation mechanisms

Cyber Security: an exercise in managing risk to the point of almost abandoning mitigating vulnerabilities

marine technology SOCIETY
Opportunity runs deep™

- Relying organizations & consulting professionals have focused on using legacy techniques & stacking redundant symmetric authentication factors to avoid meaningful change
- Security by obscurity, that has failed in the past, has once again become good enough to satisfy risk management objectives
- User Cyber Hygiene is a primary emphasis, but cyber training & awareness is less effective than physical security training due to the fact that a single malicious (or non) activity usually causes huge consequences across the entire ecosystem, worse across our trading partners & customers
- The result is that we continue to conduct business online without confidence that the online credentials being used are accurately associated with a specific entity



Bell Curve Grade Chart

Cyber training & awareness is less effective than we are accustomed to with traditional physical security training

Cybersecurity must be driven from the top

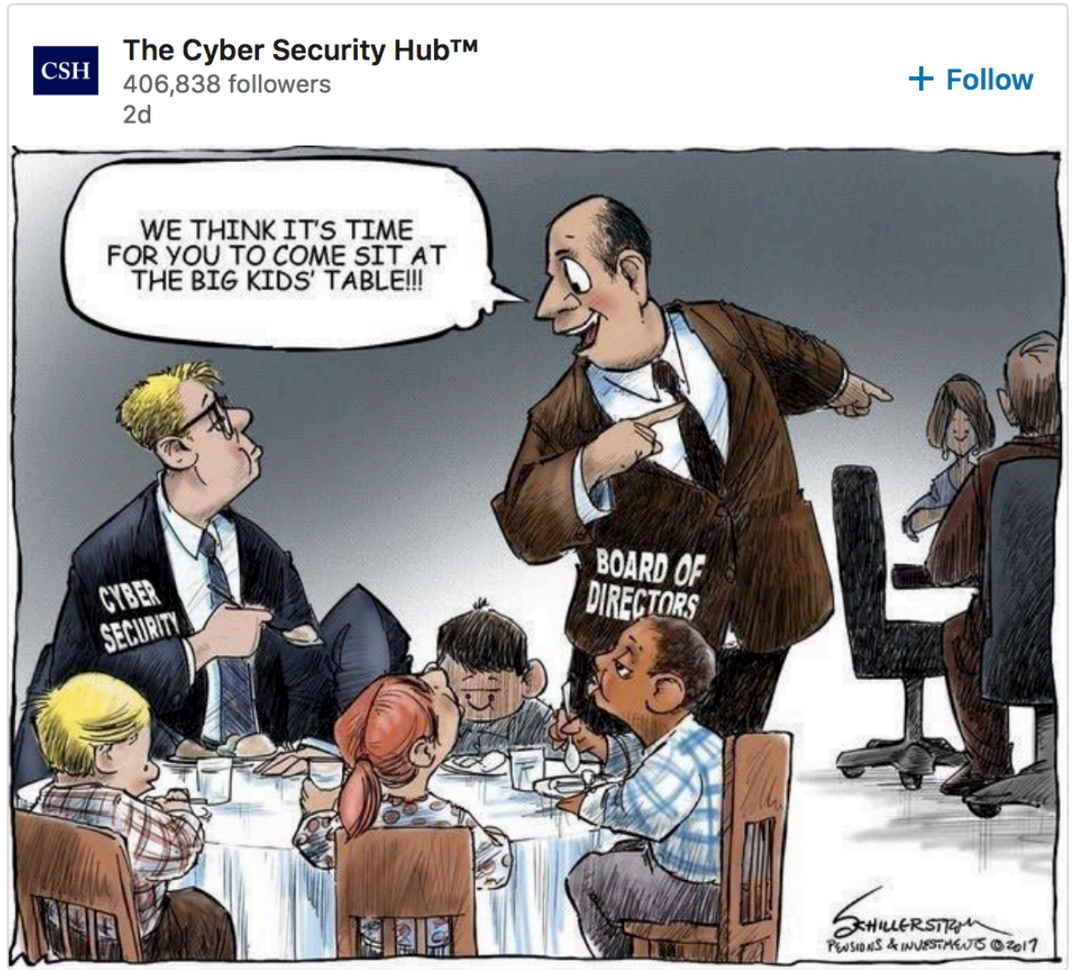
marine technology SOCIETY
Opportunity runs deep™

Address organizational impacts:

- Loss of advantage or opportunity
- Lost value/ brand
- Loss of life
- Combination of above (does not necessarily equal cost or value exactly)

Keep it Simple for Users:

- Consistent/ Unique Credentials for all Authentication
- Managed Encryption for Data at Rest, in Motion & in Process
- Practice, Practice, Practice …

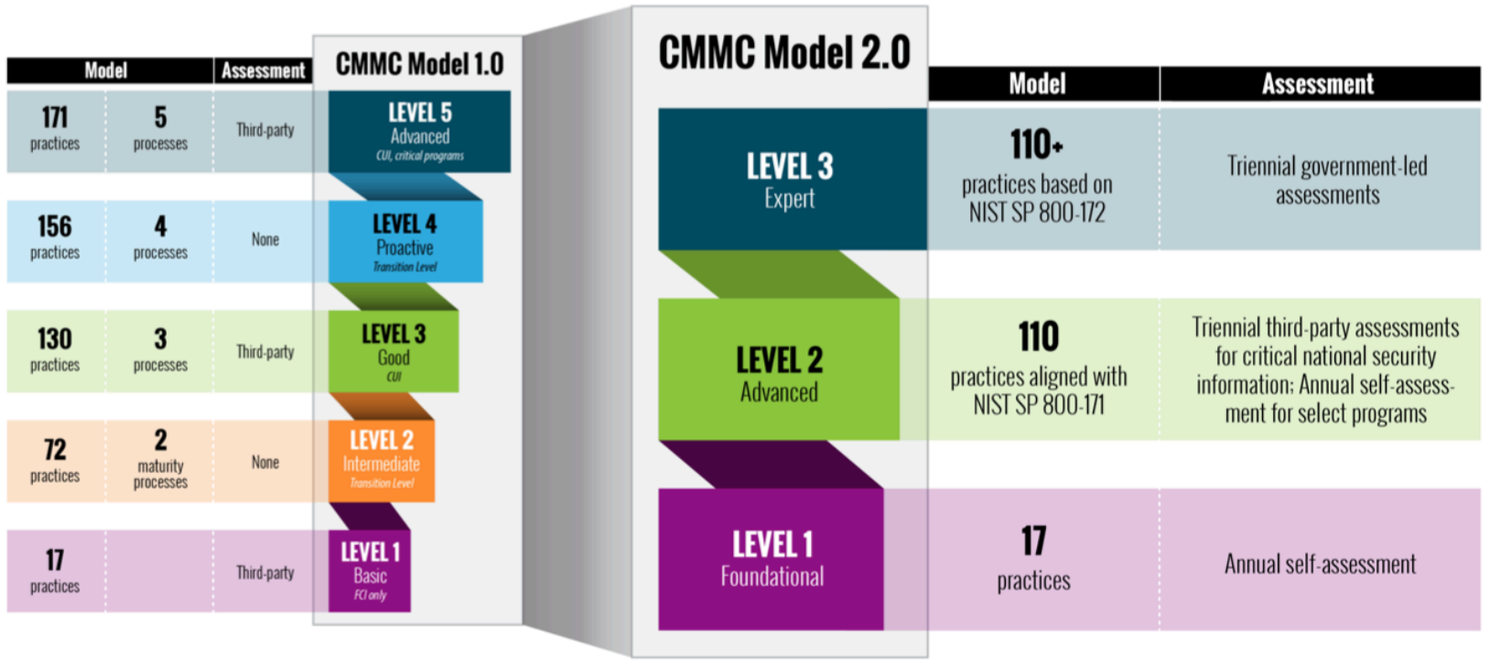


Not Just Cut and Pasted Plans

marine technology SOCIETY

Opportunity runs deep™

The CyberSecurity Maturity Model Certification (CMMC) Offers a Building Block Solution for CyberSecurity Maturity



Zero Trust Authentication & End-to-end Protection

marine technology SOCIETY
Opportunity runs deep™

Securely connect billions of end points …

… over secure communications connection …

… w/ *CLOUD/ Data Center* security built from ground up.

END POINT SECURITY

Provisioning, Registration & Authorization

CONNECTION SECURITY

X.509/TLS-Based Handshake, Strong Encryption w/ IPsec options

CLOUD SECURITY

Security Center, Directories, Key Vaults, Policy-Based Access Control

Recognize Convergence of OT & IT

Key Messages

The notion that there is no immediate preventative strategy that can curtail future Cyber attacks – is fundamentally flawed

*Smart Ships, Ports, Cities & Enterprises need to take a new **systems-based defensive approach** that eliminates human weaknesses & not pretend that the cyber problem can be solved with a simple overlay or new security monitoring & training*

*Focuses must be on interoperability, trustworthiness & privacy/ critical infrastructure protection rather then short-term **exploitation of Cyber fear***

***The Power of Simple** - enforcing strong cyber-policy & best practices without complicating the user experience, thus removing the opportunity for compromising mishaps*

We can avoid the pending Cyber Zombie Apocalypse from consuming our ability to conduct business, our national economy & defense

marine technology SOCIETY

Opportunity runs deep™

announces the new

Maritime Cyber Security and Infrastructure Committee

Cyber security has become a major issue in every industry and increasingly in military, political and financial operations. Maritime organizations represent critical infrastructure, and stakeholders in this arena include but are not limited to port authorities, terminal operators, shipping companies and various other entities that need access to the latest information, technologies, and best practices. Our members need a central resource where they can go for the latest information, advice and help when needed. The MTS Maritime Cyber Security and Infrastructure Committee will be that central resource.

marine technology SOCIETY

Opportunity runs deep™

Please Join the Conversation

Daniel E. Turissini
turissd@mac.com

Monica Ostrander
mostrander@mtsociety.org

Thank You!

Acta Non Verba!

Daniel E. Turissini
Chair, Maritime Cyber Security and Infrastructure Committee
turissd@mac.com