SOCP Cybersecurity Project Survey (2017 05-15)

Thank you for Participating in the Survey:

John Jorgensen, ABS
Chris Volkle / Matt Tucker, APL
Kyrm Hickman / Doris Locking, MSC
Mark Marien, Crowley
Cole Cosgrove, Crowley
Francis Pelosi, CSL
Bob Sheen, Ocean Shipholdings
Ann Avery, Skagit Valley College (Marine Manufacturing & Technology)

Survey Results:

#	Description	Votes	Note
1	Develop a variety of cybersecurity and resilience use cases	4	ABS has started
2	Collect cybersecurity and resilience best practices	4	(1) ABS Provides – freely available; (2) currently underway with the ASTM F25 Committee and SOCP members participating.
3	Compile cybersecurity and resilience playbooks	6	ABS has started
4	Conduct workshops and table top exercises	6	(1) ABS has started; (2) could be done in conjunction with USCG, Port Authorities, Operating Companies, Terminal Operators, the MARAD RRF and MSC along with US TRANSCOM and Cybersecurity firms.
5	Partner with US TRANSCOM as a cybersecurity commercial partner	8	(1) Suggest expanding to include partnering with the National Defense Transportation Association (NDTA) together with TRANSCOM; (2) **could be leveraged to assist with No. 4 above.**

Proposed Plan Forward:

1. Develop a Cybersecurity Standing Committee.
2. Appoint a Committee Chair (Matt Tucker, APL has volunteered; John and/or Bob might be interested as well).
3. Move forward with action item 5 & 4.
4. Place on agenda for 2018 Spring Summit (similar to Extreme Weather platform).
5. Develop a distribution list of interested participants in this standing committee, to include Mr. Dinning, members and non-members.
6. Provide resources available on the SOCP website (comprehensive list)

Resources currently available:

1. APL is in partnership with TRANSCOM – they are their largest customer and are currently working on the new TRANSCOM/NIST cybersecurity requirements for government contractors.
2. APL has a large library on this issue and is willing to share the information
3. ABS Best Practices & Other resources freely available and willing to share
4. MSC publishes a weekly Cybersecurity Newsletter that we would be willing to share with SOCP, if so desired.
5. MSC has a brief that we give CIVMARs about Cybersecurity which would be directly applicable to the mariner. This brief are actual things that they can do at their computer to protect themselves from cyber threats.
6. Ms. Locking has offered to speak to SOCP on this subject.