USE OF THE ABS FCI CYBER RISK MODEL FOR INSURANCE PURPOSES

Rick Scott, PE
10 April 2018

ABS Advanced Solutions

USE OF THE ABS FCI CYBER RISK MODEL FOR INSURANCE PURPOSES

Certification bodies and insurers are facing the same issue. We both have to predict outcomes based on our understanding of what causes loss, and collect evidence of those causes in or about the thing we are certifying or insuring. And we are both facing a situation with maritime cybersecurity that seems a bit like feeling our way in the dark. The topic is new. Solid information about cybersecurity incidents in maritime is scarce. And we aren't just concerned about dramatic failures caused by malicious intent. Those commonly make up the smaller portion of cyber incidents. We are also concerned about the greater number of non-malicious cyber incidents caused by mistakes, poor decisions, poor training, and general ignorance about the fundamental nature of cyber risk on assets and resulting losses.

When contemplating both certification of compliance and insurance covering maritime cybersecurity events, we face some interesting difficulties. Data describing cybersecurity events, incidents, and losses is highly confidential and closely guarded by the enterprises that are affected. The potential liability associated with sharing such information is unknown, sparsely defined by trial law, but perceived to be considerable. So, companies are conservative about sharing unless failure to do so increases the potential damage incurred by the event, failure to report the event, regulations, and fear of fines.

Further, cyber events that do not result in an obvious damaging incident may remain latent and go unnoticed by the impacted asset for long periods of time, and as a result go completely unreported. If the event is detected and defeated or quickly remediated, the event may go unreported completely because protections succeeded or recovery was seamless. It passes by as a job well done.

It is the fundamentals of cybersecurity risk that makes insurers and certifiers very close kin. Whether deciding if a company or asset is applying cybersecurity technology and procedures that are sufficiently reasonable and prudent for safety certification, or for providing insurance against a damaging incident, the main question is the same: Has the enterprise identified and dealt with the conditions that place the asset at risk? That single fact makes classification society engineers and insurance actuaries very close kin. We both want facts backed by quantifiable and/or observable evidence that risk is both understood and proactively managed. Assessors and insurers aren't impressed, enchanted, hypnotized by the intricacy, novelty, or apparent sophistication of threat modes and protections. Frankly, we don't even care. We just want evidence that any threat will have little or no loss or safety impact on the certified or insured asset. It's that simple – and that complicated.

When we contemplate the thousands of pages of guidance and requirements presented to cybersecurity professionals and business executives alike, a common thread emerges – and it's not even subtle. *Risk is the heart of the matter.* All guidance instructs the readers to base any "cybersecurity" process or protection activity on a *risk management plan*. In ABS certification work, this is where things pretty much begin to fall apart – which is really bad – because risk assessment is foundational and required at the beginning of a cybersecurity program standup. Risk management is the foundation of the all cybersecurity "frameworks" and implementation programs. DHS and the Coast Guard identified the issue of risk assessment as a critical gap in cybersecurity program implementation over a year ago and called on Stevens Institute and ABS to figure out what could be done about the weaknesses in (1) the general understanding of maritime cyber risk, and (2) the greater challenge to measure that risk. The resultant research work provided a way of thinking about cyber security and risk, as well as a new model for maritime operational technology risk that makes the larger idea of Risk relatively easy to understand, observe, and even measure.

The model, described in a technical paper presented by ABS at the November 2017 SNAME Maritime Convention in Houston, TX, requires application in order to be fully useful as an insurer's tool. Assets must be characterized using the model. Risk Index numbers for assets, and ultimately asset classes, must be developed. A statistically relevant number of assets in each class must be assessed and the cyber incident history for each asset must also be tracked. The Risk Index Number for each asset and its event or incident history must be documented, tracked over time, and correlated in order to establish an upper Risk Index value limit as an indicator for insurability. The Risk Index value can also conceivably be used to establish insurance rates across a range of values.

This all takes time and attention to risk event outcomes for assets that have established a Rick Index. But, it is a start and it provides quantitative information to begin to ground risk and insurance rates in empirical data. There are business and confidentiality issues to manage, but it is doable. Other asset/enterprise cybersecurity information can and should also incorporated in the insurability consideration process. Enterprise cybersecurity program attributes are arguably strong indicators of risk management due diligence.

Eventually, ABS envisions the collection of industry data that provides data-driven characterizations of entire classes of assets that can support insurer decisions. The concepts and approaches below outline possibilities for industry-wide data collection and analysis to guide insurance decisions and application of resources to cybersecurity. The industry data to be collected might include the following information to connect specific function failures with specific incident outcomes.

Information to connect Function (Consequences) failures to incident outcomes

- Identify the industrial control system (ICS) functions that are deemed to be consequential to the safety and security of the asset.
- Assess consequences of failed safety critical functions: deaths/injuries, property damage, spill, port disruption
- Map failure of safety critical functions to historical event classes
- Use historical incident data to develop distribution for each applicable impact type/asset class/ failure of a safety critical function
- Relate the impacted safety critical function to a specific Safety Integrity Levels
- Correlate cyber-initiated consequences similar to non-cyber initiated events where possible. Examples include but are not limited to:
  - Collisions/allisions/groundings
  - Fires/explosions
  - Oil spills/CDC releases
  - Loss of propulsion
  - Flooding/sinking/capsizing
  - Crane drops

Information to connect Connections (Vulnerability) to incidents

- Identify the connection types for each Asset Function as Discrete, Simple, Complex, or Very Large Network (VLN) (e.g. Internet accessible), and the access nodes by type associated with each connection.
- Map failure of safety critical functions to historical event classes
- Use historical incident data to develop distribution for each applicable impact type/asset class/ failure and correlate to connection types and nodes determined to be the entry point of the corruption causing the failure.

- Connections vary by asset class and safety critical function
  - MODUs/Drill ships highly sophisticated and connected
  - Bulk freighters less so
- Obviously, there is significant variation within a class as well based on age, service, etc.
- Develop distributions for safety critical functions and asset classes representing the percentage of the fleet with different connection types.
- More details on how to develop distribution (SME elicitation)

SAMPLE

Function	Asset Class	Simple	Discrete	Complex	VLN
Propulsion	MODU	0%	5%	25%	70%
Dynamic Positioning	MODU	0%	0%	5%	95%
Crane Control	Container Terminal	10%	90%	0%	0%

Information connecting Identities (Threat) to incidents

- Identify the digital device and human identities that can access the ICS connections and related access nodes.
- Map failure of safety critical functions to historical event classes
- Use historical incident data to develop distribution for each applicable impact type/asset class/ failure and correlate to the number of trusted and untrusted digital devise and human identities determined to have access to the entry point of the corruption causing the failure.

SAMPLE

Function	Asset Class	Trusted Device Identities	Untrusted Device Identities	Trusted Human Identities	Untrusted Human Identities
Propulsion	MODU	50%	50%	90%	10%
Dynamic Positioning	MODU	50%	50%	95%	5%
Crane Control	Container Terminal	25%	75%	50%	50%

Information connecting enterprise cybersecurity program attributes to incidents

- Determine if OT Cyber Security Office (OT-CSO) responsibilities are documented and resourced.
- Determine if Incident Response Team (IRT) responsibilities are documented and resourced.
- Determine if an OT FDD has been developed and maintained under revision management procedures.
- Determine if a compiled cyber security management system (CMS) FDD has been developed and is maintained under revision management procedures.
- Determine is Management of Change (MoC) procedure are documented and is implemented as policy.
- Determine if Cyber security training documents and programs are implemented and attendance is tracked.
- Map failure of safety critical functions to class attributes.
- Use historical incident data to develop distribution for each applicable impact type/asset class/ failure and correlate to the number attributes in place to cyber security incidents.

SAMPLE

Asset Class "Yes" Responses	CSO	IRT	OT-FDD	CMS-FDD	MOC	Training
General Cargo	20%	20%	10%	5%	15%	30%
Tanker	15%	10%	2%	2%	5%	10%
MODU	20%	20%	10%	5%	15%	30%
Tug/Barge	15%	10%	2%	2%	5%	10%
Cruise	28%	20%	18%	20%	12%	15%
Ferry	15%	10%	2%	2%	5%	10%
CDC Facility	30%	10%	2%	2%	15%	30%
Petro Facility	25%	10%	2%	2%	15%	30%
Cargo Terminal	35%	10%	2%	2%	15%	30%
MTSA 106 Facility	35%	10%	2%	2%	15%	30%

These concepts provide clearly understandable "knobs to turn" for cybersecurity practitioners, program managers and senior executives. The concepts are simple in concept, but sophisticated in application. They respect the long-developed and accepted principles of cyber security, and frame those principles in a simple, memorable model for specific application to maritime cybersecurity situations. They acknowledge engineering principles by resolving real world constructs numerically so that they can be better understood and made more predictable and reliable. They provide a technique for assigning quantitative relative sufficiency to Operational Technology (OT) cyber security systems and a method for measuring system improvement. But most importantly, the concepts provide potential for a uniformly accepted practical approach to assessing maritime Risk.

CONTACT INFORMATION

WORLD HEADQUARTERS
16855 Northchase Drive
Houston, TX 77060 USA
Tel: 1-281-877-6000
Fax: 1-281-877-5976
Email: ABS-WorldHQ@eagle.org
www.eagle.org

AMERICAS DIVISION
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA
Tel: 1-281-877-6000
Fax: 1-281-877-5943
Email: ABS-Amer@eagle.org

EUROPE DIVISION
ABS House
No. 1 Frying Pan Alley
London E1 7HR, UK
Tel: 44-20-7247-3255
Fax: 44-20-7377-2453
Email: ABS-Eur@eagle.org

GREATER CHINA DIVISION
5th Floor, Silver Tower
No. 85 Taoyuan Road
Huang Pu District
Shanghai, 200021 P. R. China
Tel: 86-21-2327-0888
Fax: 86-21-6360-9649
Email: ABS-GreaterChina@eagle.org

PACIFIC DIVISION
438 Alexandra Road #10-00
Alexandra Point
Singapore 119958
Tel: 65-6276-8700
Fax: 65-6276-8711
Email: ABS-Pac@eagle.org