



IUMI 2018

Should you worry about the cyber risk to cargo?

Rod Johnson
RSA Global Risk Solutions
September 2018

Cyber is not a peril

Consider the usual perils for marine cargo, goods in transit and stock throughput policies. Cyber isn't there.

It is unhelpful to think about cyber as a separated peril or issue – in fact it's an integral part, or feature, of the world we live in.

Cyber is a new pathway to conventional loss, and our apprehension of it comes from our collective lack of understanding of the issues.

Cyber as a pathway is harder to detect and pushes discovery and remediation into the future.

Sales people leverage this and use fear based marketing, amplifying the uncertainty

Cyber is a dual use technology



And it makes the
global supply chain
work.

How?

By removing
friction

Friction

Any point in a process where a manual intervention is required or unavoidable.

Interventions take time and accumulate into delays.

Interventions have the potential to either introduce error or detect it.

Software designers and integrators look to make cyber enabled processes as frictionless as possible. That's Good Cyber if there are sufficient checks and balances.

Bad Cyber doesn't have those checkpoints, which is why it takes longer to detect losses or even understand what has happened or what has been lost.

Bad Cyber effect of standard perils

- Fire and explosion
- Grounding or stranding of the vessel
- Jettison of the cargo
- Sinking
- Collision
- Damage to the cargo if it has to be discharged after damage to the ship
- Washing overboard
- Entry of sea, lake or river water to the vessel or place of storage
- Total loss of a package by falling overboard
- Theft, pilferage and non-delivery
- Storage risks
- War and strikes risks
- Malicious damage

Effective risk management – know the problem



The Cascade Effect

- Charterers sub contractors
- Freight forwarders
- Sub sub contractors
- Your global head office
- Terminal operators
- And who else?

Aggregation and accumulation!

Effective risk management – underwriter due diligence

Understand the pathways to loss, modes of attack, vulnerabilities, high risk activity, market conditions and imperatives

Quiz the client and the broker – compliance with the “10 Steps”, supply chain integrity, supply chain partners

Understand that the claims record may have some latency and anyway the past does not inform the future – what’s the real risk?

Always consider engaging your in house risk consultants. Haven’t got any? Get some. A basic cargo focused team will cost you less than one mid size claim per year.

Effective risk management – advising the assured



10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



Network Security

Protect your network from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.



User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.



Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.



Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.



Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.



Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.



Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.



Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.



For more information go to www.ncsc.gov.uk @ncsc



CONCLUSION

Cyber is a dual use technology and an inescapable fact of life, so embrace it

Bad Cyber presents new and obscure pathways to loss

Bad Cyber drives latency into loss detection

Bad Cyber always affects more than one part of the supply chain

Defence is simple and straightforward but not yet normalised into business

THANK YOU

Rod Johnson
rod.johnson@uk.rsagroup.com
September 2018

