RUSSIA/UKRAINE WAR AND ANTICIPATED INCREASE IN CYBER ATTACKS

Maritime Mutual Risk Bulletin No. 56

March 28, 2022

INTRODUCTION

As a consequence of the Russia/Ukraine war and the financial sanctions being imposed on Russia, shipping companies, flag states and other players in the maritime industry may see an increase in cyber-attacks aimed at companies from the sanction imposing countries. This Risk Bulletin is focused on the disruptive and costly impacts which these targeted cyber-attacks may have on MM Members and their shore-based and shipboard operations as a consequence of indirect/collateral damage.

BACKGROUND

Members have already been alerted to the dangers of cyber-attacks and the necessity for proactive loss prevention by Risk Bulletin (RB) No. 29 for May 2020. This RB included references and links to IMO Guidelines and Circulars on Maritime Cyber Security Management and the International Chamber of Shipping (ICS) Guidelines on Cyber Security on Board Ships, Version 3, Dec 2018.

RB No. 29 also highlighted the IMO imposed obligation to ensure that processes for the control of cyber risks are incorporated into ISM Code SMS manuals and procedures no later than the first annual verification of each ship's Document of Compliance after 1 Jan 2021. It should now be the case that all SMS manuals and procedures for vessels regulated by SOLAS, or similar NCVS regulation for vessels in domestic trade, have been updated to include the control of cyber risks and have been approved as such by their flag states.

Although not specifically referred to in RB No. 29, it should be noted that ISPS Code Ship Security Plan (SSP) must now include information on the management and control of cyber risks. This should be accomplished by the creation of a supplementary Cyber Security Plan (CSP). The CSP should then be cross-referenced to the cyber-security information contained in the SMS. More information on the ISPS Code aspects of cyber-security is provided below.

LESSONS LEARNED – MAERSK AND THE 2017 'NOTPETYA' ATTACK

Members will probably be aware that, during the past decade, the Russian government, or unidentified criminal 'hackers' within Russia, have been cited as being responsible for a significant number of global and costly cyber-attacks on both governmental and commercial organisations. The most well known of these incidents appears to have been the 'NotPetya' attack which occurred in 2017.

The 'NotPetya' attack – which was a malicious code or 'worm' attack designed to destroy data – targeted Ukrainian government and financial entities as well as transport systems. It caused financial and transport chaos. However, due to what is known as 'spill over' effect into the internet, it ultimately impacted computer systems across the globe. This included Maersk Lines, at that time the world's largest container line.

The global cost of the 'NotPetya' attack was estimated to have run to over USD 10 billion. Maersk's Active Directory network was crippled within seven minutes. Most of the damage was done within an hour. It then took nine days and hundreds of Maersk personnel to restore its systems. The indirect/collateral damage cost to Maersk was estimated at about USD 300 million.

The lesson to be learned here is that Maersk was not targeted directly. Despite this, their systems were attacked by a 'worm' which had been maliciously implanted in a website update for a Ukrainian Government tax website. All that was required was for someone in a Maersk office to download the infected update and, within minutes, it would then spread through their entire system. Evidently, this is precisely what occurred at Maersk and, globally, at numerous other untargeted government and commercial entities which were also very seriously impacted.

CYBER-ATTACKS AND CYBER-BREACHES ON MM MEMBER VESSELS

Members who operate smaller vessels may believe that their shipboard IT (Information Technology) and OT (Operational Technology) systems are too basic to generate any significant cyber security risks. However, these risks can exist on board even small coastal ships and tugs where IT system shipboard computers and OT systems, such as GPS, AIS and ECDIS units, can be inadvertently infected. Common examples include:

- Insertion of a Malware infected USB or Internet connection to an infected shoreside IT system by an attending technician for OT system updating or patching purposes.
- Insertion of an infected USB into a shipboard computer by ships agents, customs officers or other persons for document printing purposes.
- Use of a bridge OT system plug to recharge a crew member's Malware infected mobile phone.
- Inadvertent downloading of a Malware virus during Internet connected use of shipboard computers for communication or data download purposes.

Two short videos which illustrate the examples above and the potentially serious outcomes are available at the links below.

Be Cyber Aware at Sea, NSSL Global

Cyber Security Awareness in the Maritime Industry, DNV GL

CURRENT MARITIME CYBER SECURITY MANAGEMENT BEST PRACTICE

Members are advised that an update of the ICS Guidelines, now the ICS Guidelines on Cyber Security on Board Ships, Version 4, was published in Dec 2020 (six months after Risk Bulletin No 29 was posted). As before, the ICS Guidelines may be downloaded free of charge.

The updated ICS Guidelines contain 10 detailed sections, inclusive of real-life case examples. These sections start with an explanation of cyber security fundamentals, move on to explaining assessment and procedures and finish with the process of response and recovery from a cyber security incident. There are also 5 Annexes which provide supporting detail. In short, the ICS Guidelines provide essential 'industry best practice' reading for Members, their DPA's, CSO's and Masters.

Members should also download a copy of the free publication, Code of Practice: Cyber Security for Ships, published by the UK Dept. of Transport in 2017. The Code contains a wealth of cyber-security information which has been written specifically for shipboard use. It focuses on the ISPS Code security requirements and the incorporation of cyber security into this system by first conducting a Cyber Security Assessment and then creating and implementing a Cyber Security Plan. Again, this Code should also be considered as essential loss prevention reading.

CONCLUSION AND TAKEAWAY

At the time of writing this Risk Bulletin, the conflict between Russia and Ukraine continues. The only positive aspect is that negotiations between the parties continue and there are indications that a peace agreement may ultimately be accomplished. However, even if this should occur, sanctions against Russia may remain in place for some time and the current heightened cyber-attack risk may well continue for many months, if not years.

In addition to the cyber-security recommendations provided in Risk Bulletin No. 29, MM now encourages all of its Members to upgrade their cyber-security defences to meet the current and heightened risk of a cyber-attack, whether targeted/direct, indirect/collateral or inadvertent/accidental, by taking the following steps:

1. **Raise Awareness** by ensuring that their ship managers, DPAs, CSOs and masters are provided with a copy of this Risk Bulletin.

2. **Update ISM Code SMS Manuals** by instructing their ship managers and DPAs to check that the SMS Manuals and Procedures for all of the vessels in their fleet have in fact been updated to include the IMO requirements for cyber-security. Documents which should be specifically referred to in those Procedures and attached or linked to them include:
    - IMO Res MSC.428(98) and MSC-FAL.1/Circ.3
    - ICS Guidelines on Cyber Security on Board Ships, Version 4
    - Code of Practice: Cyber Security for Ships
3. **Update ISPS Code Security Plans** by similarly checking that all Ship Security Plans (SSPs) and associated documentation have been updated to include Cyber Security Plans (CSPs) and that CSPs are cross-referenced to SMS Manuals and Procedures.
4. **Instruct DPAs and CSOs** to ensure implementation of all recommended cyber-security practices on board all vessels in the Member's fleet during all shipboard attendances and especially during ISM Code and ISPS Code auditing processes.
5. **Encourage Masters** to discuss the dangers of cyber-attacks and the use of cyber-security industry best practices with officers and crew at the next monthly shipboard safety meeting.