19th Annual General Assembly – AGA 2018
International Association of Maritime Universities (IAMU)
M. Grifoll, F.X. Martínez de Osés, M. Castells and A. Martin **(Eds)**

A FRAMEWORK FOR CYBER SECURITY RISK ASSESSMENT OF SHIPS

BORIS SVILIČIĆ[*], JASMIN ČELIĆ[*], JUNZO KAMAHARA[†] AND JOHAN BOLMSTEN[††]

[*] Faculty of Maritime Studies
University of Rijeka
Studentska ulica 2, 51000 Rijeka, Croatia
e-mail: svilicic@pfri.hr, https:// www.pfri.uniri.hr

[†] Graduate School of Maritime Sciences, Kobe University
5-1-1 Fukaeminami-machi, Higashinada-ku, Kobe, Japan
e-mail: kamahara@maritime.kobe-u.ac.jp, web page: http:// www.maritime.kobe-u.ac.jp

[††] World Maritime University
Fiskehamnsgatan 1, 211 18, PO Box 500, SE-201 24, Malmö, Sweden
e-mail: johan.bolmsten@wmu.se, web page: http://www.wmu.se

Keywords: maritime traffic, maritime cyber risk management, ship cyber critical systems, cyber risk assessment, assessment framework.

Abstract. In maritime traffic, with the growing reliance on innovative ICT technologies, maritime cyber risk management to secure not only data, but as well as safe and reliable ship transport operations becomes increasingly important. This paper presents a framework for conducting general and comprehensive cyber risk assessment of ships to offer guidance for improving security level of cyber systems onboard ships. The assessment covers methods for identification of the both technical and administrative cyber threats and vulnerabilities, and relies on identification of ship cyber risk critical systems and assets. The vulnerability scanning and penetration testing as specific elements of ships cyber security assessment have been studied. The given methodology for cyber risk level determination is based on a qualitative approach to assessing risk.

1 INTRODUCTION

Ships are increasingly using information technology and operational technology systems that both rely on digitalization, integration, automation and networking. With growth in reliance on the information and communication technologies (ICT), there is a compelling necessity to develop mechanism and measures that allow not only data protection, but as well as safe ship operations [1-9]. Recently the International Maritime Organization (IMO) has published the

Guidelines on high-level recommendations for maritime cyber risk management [10]. While maritime regulations and policies currently do not adequately govern cyber security in the same way as other aspects of ships security and safety, cyber security risk assessment can be considered as being partly regulated by the IMO ISPS Code [11]. However, IMO has imposed to include maritime cyber risk management in the ISM Code safety management system on ships by 1st of January 2021 [12].

In this work, we present a framework for conducting cyber risk assessment of ships to offer guidance for improving security level of cyber systems onboard ships. As for ship uniqueness (in design, operations, cargo, operating environments...), the framework presented provides a method to balance appropriate cyber security mechanisms and measures by evaluating ship critical cyber systems and assets, key shipboard operations, existing safeguard controls, assessed cyber threats and vulnerabilities, and determined risk level.

2 CYBER RISK ASSESSMENT FRAMEWORK

A systematic cyber risk assessment is an essential part of the process for cyber security improvement of ships. Ship cyber risk assessment is a complex set of related and interdependent actions that intersect so as to provide safeguards that are effective and corresponding to challenges presented by ship critical systems specifics, ICT technologies evolution, and human resource capabilities. Cyber risk assessment relies upon determination of ship specific cyber risk factors to be assessed and relations among those factors. Results should provide identification of threats and vulnerabilities in the current deployment of ship critical systems and determination of likelihood and impact magnitude of their exposure caused not only by hardware or software, but also by implemented operational procedures and security policies.

The developed framework that relies on guidelines and practices [10-15] is shown on Figure 1. Framework consist of four main segments: (i) assessment preparation operations including ship critical systems identification, (ii) current cyber security assessment conduction and cyber risk determination, (iii) assessment results communication activities necessary for cyber security level improvement, and (iv) cyber risk assessment maintenance activities for ensuring efficiency. The proposed framework is not intended for initial assessment only, but also for periodic implementation to respond to rapid technological changes in a ship environment.

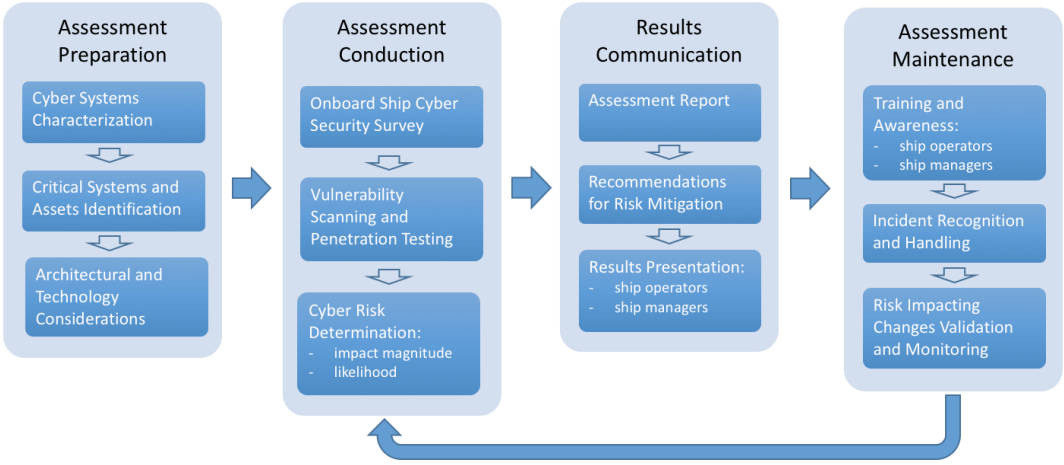

Figure 1: Proposed framework for cyber security risk assessment of ships

3 ASSESMENT PREPARATION

The first phase to be performed as a part of the assessment is characterization of the ship cyber systems by gathering information about ship general technical specifications (type, layout of the ship, stowage arrangements plan...), identifying critical operations (cargo operations, crew/passenger exchange, bunkering...), identifying critical arears and personnel that may be targeted in cyber security incidents, and identifying possible types of motives for cyber security incidents (economical, political, symbolic, terroristic...). The outputs from the system characterization is basis for identification of ship cyber risk critical systems and assets. The Figure 2 shows general overview of ship cyber risk critical systems and assets.

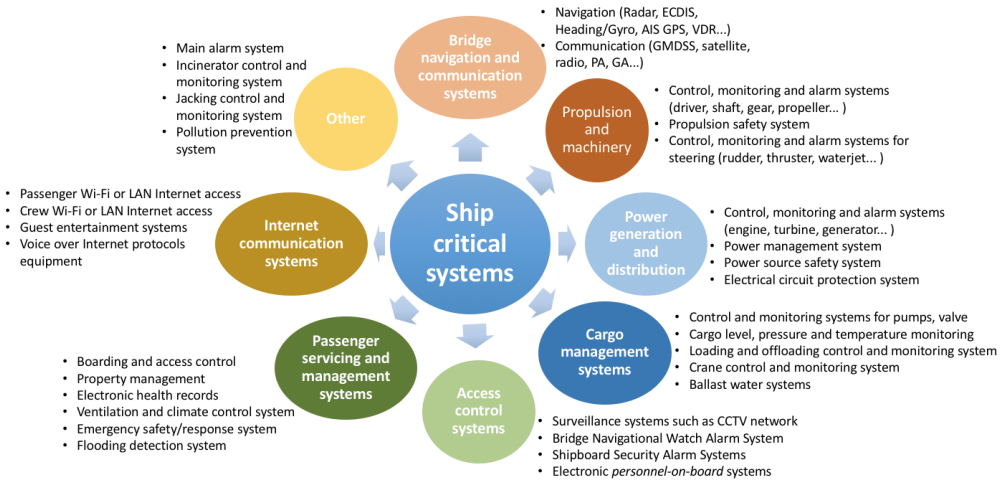

Figure 2: Ship cyber risk critical systems and assets

A comprehensive identification of the ship cyber risk critical systems and assets strongly depends on key shipboard operations being performed on a particular ship, such as navigation in high density traffic area, navigation in restricted visibility, heavy water operation, people accessing the ship... The next step is to consider the technological and architectural implications of the identified critical systems/assets on the cyber security, e.g. implemented network connections, operating systems, services, applications...

4 ASSESMENT CONDUCTION

Onboard ship cyber security risk assessment conduction consists of three main actions: (i) onboard ship cyber security survey performing, (ii) vulnerability scanning and penetration testing, and (iii) cyber risk level determination.

4.1 Ship cyber security survey

The goal of performing and documenting the ship cyber security survey is to confirm that cyber security safeguard mechanisms and measures assumed to be in place and to identify non-existing and/or insufficient safeguard mechanisms and measures. To collect the relevant information, a questionnaire concerning the ship managers and operators is developed on the basis of the ship cyber risk critical systems and assets identified. The evaluation of current cyber security safeguard mechanisms and measures allow identification of eventual cyber threats and vulnerabilities. An example of a questionnaire for conducting the survey by interviewing the ship crew is given in Table 1.

Table 1: Example of cyber threats and vulnerabilities survey

Critical System	Assets	Threats	Vulnerabilities
Cyber security management system	Policies and procedures	- Policies and procedures related to cyber security are developed - Policies and procedures are communicated to the all crew...	- Roles and responsibilities are not clearly defined - Incidents detection, analysis and response...
	Incident handling and response management	- All information security incidents are reported - Mechanism to monitor and quantify incidents is identified...	- Roles and responsibilities are not clearly defined - Incidents detection, analysis and response...
	...	...	...
Bridge Systems	ECDIS	- Communication security - Software security...	- Connections to the Internet is established - Operating system and applications are patched...
	ARPA	- Cyber incident handling procedures are in place - Handling of portable devices...	- Incidents detection, analysis and response - Enforcement of security status of USB media...
	...	...	...
Propulsion and machinery management and power control systems	Control and monitoring system	- Access controls are in place - Authentication controls are in place...	- All accesses are provided to authorized personnel only - All control mechanisms are enforced...
	Alarm system	- Audit and logs are in place... - Procedure for authorized access...	- Security-relevant events are recorded and kept - Log-out obligation is enforced...
	...	...	...
Cargo management systems	Remote control and alarm systems for pumps	- Remote authentication controls are in place - Physical access is provided to authorized personnel only...	- Remote authentication by using cryptographic only - All default passwords have been changed...
	Conditioning, temperature, ventilation system of cargo	- Policies and procedures are reviewed periodically - Training before actual use of a program...	- Incidents detection, analysis and response - Physical and environmental protection...
	...	...	...
Passenger servicing and management systems	Ventilation and climate control system	- Access control policy - Fail-over procedures	- Documentation of authorized users and privileges - Redundant architecture and backup systems...
	Flooding detection system	- Policy for authorized access - Training on security safeguards...	- Password sharing and common accounts are forbidden - Incident recognition and handling...
	...	...	...
Internet communication systems	Firewall	- Network privacy protection - Latest patches or new releases are implemented...	- Firewall designs, rules and policies - Central management and reporting...
	Anti-virus software	- Malicious code protection mechanisms are implemented - Latest virus definitions or new releases are implemented...	- Malicious software infections - Central management and reporting...
	...	...	...
...	...	...	...

4.2 Vulnerability scanning and penetration testing

Compared to other types of ship assessment [15], the most specific element of the cyber security risk assessment is conduction of vulnerability scanning and penetration testing. The vulnerability scanning is a process of reviewing critical systems and assets to locate and identify known weaknesses. As a step beyond, penetration testing is a systematic employment of legal and authorized attempts to exploit target system/asset in order to prove that a cyber risk exists. Therefore, in this work, vulnerability assessment is considered as an phase utilized to complete a process of penetration testing. Process for conducting vulnerability scanning and penetration testing (Figure 3) starts with gathering all relevant information about the target system. This phase relies on the data collected by the survey, which should be enhanced with technical documentation of the target system. The second phase of the process begins by breaking the model preparation for effective scanning and testing into three distinct steps: (i) determining turned-on and communicable target systems, (ii) identifying active ports and services on the target system, and (iii) obtaining appropriate credential to gain access to the targeted system.

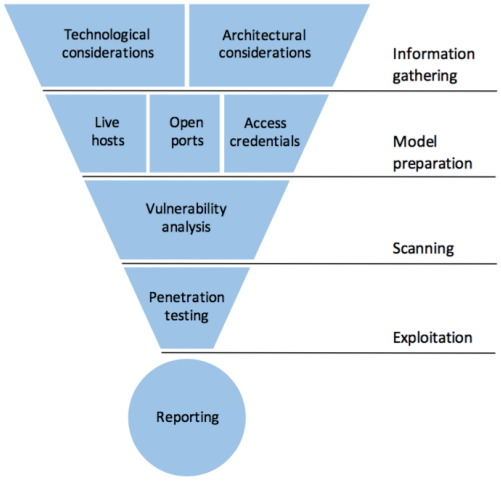

Figure 3: Process for conducting vulnerability scanning and penetration testing

Vulnerability scanning and penetration testing, the third and fourth phases, in information systems generally is mainly conducted using commercial tools (Table 2). The main advantage is ability to scan a large number of hosts for common vulnerabilities and exposures. However, the process is limited to only detecting vulnerabilities and exposures for which the vendor of the tool used has released plugins. In addition, as the tool vendor has no knowledge of a ship critical systems and assets specifics, the results could incorrectly reflect the real risk.

Table 2: Vulnerability scanner (VS) and penetration (PT) test software tools

Name	Type	License	Operating System
Nessus	VS & PT	Proprietary	Cross-platform
Kali	VS & PT	GPL	Linux
ImmuniWeb	VS & PT	Proprietary	MS Windows
Netsparker	VS & PT	Proprietary	MS Windows
Acunetix	VS	Proprietary	Cross-platform
Nexpose	VS & PT	GPL	Cross-platform
Core Impact	VS & PT	Proprietary	MS Windows
OpenVAS	VS	GPL	Linux
Retina	VS	GPL	MS Windows

4.3 Cyber risk determination

On the basis of the assessment results, cyber risk analysis is performed to identify and categorized cyber threats to which an ship is exposed. The qualitative risk analysis is performed by evaluating the impact magnitude and likelihood of various threats determinated that could exploit vulnerabilities to harm cyber security of critical systems and assets. The method provides a relatively simple, but satisfactory bases for the cyber risk analysis. The threats likelihood is a rating of the probability that a vulnerability is exploited. The likelihood levels are given as low, medium and high with given values of 0.1, 0.5 and 1, respectively (Figure 5). The impact refers to the magnitude of a harm resulting from successful exploitation of a vulnerability. The impact magnitude rates are high, medium and low with given values of 100, 50 and 10, respectively.

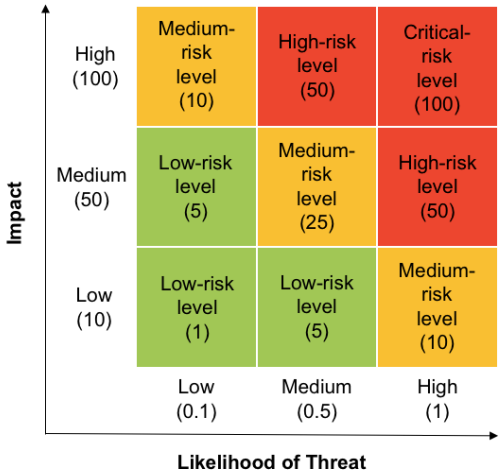

Figure 4: Example of risk-level matrix for qualitative risk analysis of cyber threats

Cyber risk level is calculated by multiplying the threat likelihood ratings by the impact magnitude of the vulnerability exploited. The given result indicates qualitative risk level: (i) critical-risk level requiring immediate action, (ii) high-risk level requiring remediation implementation plan, (iii) medium-risk level which may be acceptable over the short period of time, and (iv) acceptable low-risk level.

5 RESULTS COMUNICATION AND ASSESSMENT MAINTENANCE

The final steps in the cyber risk assessment process are the results communication and assessment maintenance. The assessment results communication phase produces assessment reports that describes cyber threats and vulnerabilities, qualitative risk level determined and recommendations for implementation of safeguard controls to mitigate the cyber risks. The report is to ensure that each recommendation is addressed with specific, realistic, and tangible actions. The recommendations should contain information to support appropriate decisions on ship policies, procedures, operational impact and feasibility. Because a cyber risk can never be completely eliminated, recommendations for the risk mitigation must be acceptable by a cost-benefit analysis, resulting in a least-cost solution with minimal adverse impact on the ship critical systems and assets. The assessment report is presented to the ship managers and operators to improve the cyber security level.

The whole ship's crew cyber security awareness and training have a significant impact on detecting cyber security incidents and preventing cyber security compromises in general. So, it is considered as a part of the assessment maintenance phase. The whole ship's crew has the obligation to be aware of their responsibilities in protecting the critical systems and assets from compromise. In addition, ship crew training is also a tool that can increase ship's crew awareness and capabilities in recognition and handling of cyber security incidents. Incidents prioritization is very important for successful response process and is conducted on the basis of the determined risk-level matrix (Figure 4). During incident handling, communication with external parties is required (vendors, law enforcement, media...), so communication guidelines are predetermined to share only appropriate information with the right parties.

Once the cyber security risk assessment of a ship has been completed and recommendations for the risks mitigation are initiated, the achieved risk impacting changes are validated and monitored. The validation and monitoring processes basically include the activities covered with the assessment conduction phase (onboard ship cyber security survey, vulnerability scanning and penetration testing, and the risk determination) resulting in updated recommendations for risk mitigation. Therefore, the cyber security management requires continuous commitment, evaluation and improvement of the safeguard controls to mitigate the cyber risks.

6 CONCLUSIONS

A general and comprehensive framework for conducting cyber risk assessment of ships is presented. The assessment covers methods for identification of the cyber threats and vulnerabilities caused by installed hardware or software, as well as by implemented security policies and operational procedures. The assessment relies on the identification of ship cyber critical systems and assets that strongly depend on key shipboard operations being performed on a particular ship. As a part of the process for the identification of cyber threats and vulnerabilities, a questionnaire for conducting the survey by interviewing the ship crew to evaluate current implementation of cyber security safeguard mechanisms and measures is presented. In addition, the vulnerability scanning and penetration testing, as a specific element of ship cyber security risk assessment, are studied. The qualitative cyber risk analysis based on the of risk-level matrix is proposed. The presented study provides guidelines for mitigating the cyber risks and to improve the cyber security level of ships.

ACKNOWLEDGMENTS

The research was financially supported by the Faculty of Maritime Studies University of Rijeka under the research project Internet of Maritime Things and Cyber Security.

REFERENCES

[1] Lee, Y.C., Park, S.K., Lee, W.K. and Kang, J. Improving cyber security awareness in maritime transport: A way forward. *Journal of the Korean Society of Marine Engineering*. Korea: Korean Society of Marine Engineering, 2017, 41 (8), 738-745. ISSN 2234-7925.

[2] Sviličić, B., and Kraš, A. Computer Systems Privacy Protection. *Journal of Maritime Research Pomorstvo*. Rijeka: University of Rijeka Faculty od Maritime Studies, 2005, 19

(2), 275-284. ISSN: 1332-0718.

[3] Hassani, V., Crasta, N. and Pascoal, A.M. Cyber security issues in navigation systems of marine vessels from a control perspective. In: *Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering - OMAE*. New York City: American Society of Mechanical Engineers, 2017, pp. 1-6. ISBN: 978-079185774-8.

[4] Polatid, N., Pavlidis, M. and Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards and Interfaces*. Amsterdam: Elsevier B.V., 2018, 59, 74–82. ISSN: 09205489.

[5] Hareide, O.S., Jøsok, Ø., Lund, M.S, Ostnes, R. and Helkala, K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*. Cambridge: Cambridge University Press, 2018, in press. ISSN: 03734633.

[6] Shapiro, L.R., Maras, M.-H., Velotti, L., Pickman, S., Wei, H.-L. and Till, R. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Journal of Transportation Security*. New York: Springer, May 2018, 8, 1–19. ISSN: 19387741.

[7] Botunac, I. and Gržan, M. Analysis of software threats to the automatic identification system. *Brodogradnja*. Zagreb: Brodarski, May 2018, 68 (1), 97–105. ISSN: 0007215X.

[8] Burton, J. Cyber attacks and maritime situational awareness: Evidence from Japan and Taiwan. In: *Proceedings of the 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. New Jersey: Institute of Electrical and Electronics Engineers Inc., 2016, pp. 1-4. ISBN: 978-150900703-5.

[9] Balduzzi, M., Pasta, A. and Wilhoit, K. A security evaluation of AIS automated identification system. In: *Proceedings of the 30th Annual Computer Security Applications Conference*. USA: Association for Computing Machinery, 2014, pp. 436-445. ISBN: 978-1-4503-3005-3.

[10] International Maritime Organization. MSC-FAL.1/Circ.3: Guidelines on maritime cyber risk management. London: IMO, 2017

[11] International Maritime Organization. SOLAS/CONF.5/34: International Ship and Port Facility Security (ISPS) Code. London: IMO, 2013

[12] International Maritime Organization. MSC 98/23/Add.1: Maritime Cyber Risk Management in Safety Management Systems. London: IMO, 2017

[13] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2014

[14] The European Maritime Safety Agency, M. Mylly. High Level Conference on Cyber Security in Civil Aviation: Cyber Risks in Maritime Community. Krakow: EMSA, 2017

[15] DNV GL. DNVGL-RP-0496: Cyber security resilience management for ships and mobile offshore units in operation. Oslo: DNV-GL, 2016

[16] Ernstsen, J. and Nazir, S. Consistency in the development of performance assessment methods in the maritime domain. *WMU Journal of Maritime Affairs*. New York: Springer, 2018, 17, 71–90. ISSN: 1651-436X.