CYBER THREAT IN MARITIME INDUSTRY – SITUATIONAL AWARENESS AND EDUCATIONAL ASPECT

Capt. (N) (r) Professor D.Sc. Kiril Kolev
Capt (N) Nedko Dimitrov, Assoc. prof. PhD
Nikola Vaptsarov Naval Academy, Varna, Bulgaria
n.dimitrov@nvna.eu

Abstract This paper examined a variety of important educational issues, management practices, and information technologies related to cyber security. The field of cyber security is more important than ever for any one maritime organization and related companies in the supply chain. As well government organizations and law enforcement agencies have to work with private companies to share, communicate, and collaborate in solving technical and human issues in this field. If all the personnel are well prepared in the cyber security domain according to the responsibilities and duties this will raise the level of cyber security awareness, alert, and readiness for action.

Based on the content analysis of the curriculum of the specialties at Maritime University NVNA, Varna and identified cyber threats and means to impose them in maritime domain the authors suggested new approach to enhance not only the education of cyber security expert and manager but all the personnel involved as an users of communication and information systems supporting the business processes of the maritime companies/infrastructures.

Exploring the statistics of cyber incidents, such as information losses, theft, and malware propagation causes business failure the authors bring their attention to the human factor in cyber security. For solving the issue with the highest percentage of cyber incidents causer they reach the conclusion that it is vital to stress not only to the technical part of cyber security and prepare well educated administrators and managers but to pay significant attention to every one user of the information systems used in navigation and maritime business.

Key words: Cyber security, cyber threat, human factor, education, curriculum

Introduction

Today's modern cyber commerce-based industries such as the navigation and maritime industry are faced with increased global competition and increased physical and cyber security threats, while simultaneously striving to increase value in the value chain. Since the 1970s information and telecommunication systems have provided business many benefits in the field of commerce, such as:

- Increased efficiency of core business process (e.g., human resources/staffing, payroll, accounting, etc.);
- Improved information sharing between trading partners (e.g., importers/exporters, shipping companies, charterers, agents/representatives, custom brokers, and government authorities); and
- Enhanced communications between administrative employees, manning organizations, and vessel personnel.

The field of cyber security and assurance is complex and challenging, as it involves many human ant technical aspects of security. To strengthen the cyber security is not only technical but mainly human issue.

The authors raise the thesis that to enhance the level of cyber security it is necessary to stress on human factor and particularly to conduct proper education of all the regular users of the information systems implemented in the navigation and maritime business.

1. Human factor in a maritime company cyber security

The history of cyber security is closely linked to the field of computer security and has its roots in World War II. During this conflict, the British and U.S. militaries had various programs to intercept and crack the communications of the German and Japanese forces. In fact, some historians argue that this was the only way that the United Kingdom and the United States gained an advantage over its adversaries.

In the mid-1990s, one of the major results of the Year 2000/Millennium Bug crisis was the growth of *enterprise resource planning* (ERP) systems. Instead of rewriting or otherwise fixing thousands of lines of programming code in their various applications, many organizations found it more efficient to replace their legacy systems with ERP systems. During this time, products such as SAR R/3, PeopleSoft, JD Edwards, Baan, and Oracle Financials became very popular, particularly in large global companies.

One of the concerns with ERP systems is the tight integration of the individual software modules (e.g., human resources, payroll, accounts payable, etc.). Practically, to implement these systems before January 1, 2000, some of these projects were done very quickly. ERP systems are known to be highly complex. Therefore, the security aspects of these systems are complicated.

Database security is yet another facet of cyber security. The main issues within this area typically involve restricting access control and limiting file updates and retrieval mechanisms and powerful user privileges. Individual user rights need to be appropriately restricted based on job duties. Retrieval methods should also be tightly controlled to prevent accidental or intentional data corruption and theft.

Application security is concerned with detailed security configuration and parameters within a specific software product such as the International Maritime Organization's Global Integrated Information System. This type of security is highly dependent on the security features and capabilities that were built into the software when it was developed. For instance, some applications allow for detailed security settings, whereas others do not. Application security typically covers such important features as access controls, transaction processing, and file permissions (i.e., read/write, modify, read only, delete, etc.).

Maritime organizations operating in the electronic commerce environment face various vulnerabilities. The first common vulnerability is errors which are intentionally mistakes by personnel. For example, an employee might accidentally input the wrong financial figure in an electronic spreadsheet, and a manager then uses this information to make an incorrect business decision. The second common vulnerability is fraudulent acts, which might involve collusion with other employees (e.g., both information systems and non-information systems) as well as outsiders. Reputational risk is another important risk to address. One information security incident such as defacement of the company's website could have an important impact on the company's general reputation in the industry. Business interruption is the final common technical threat which deals with the financial consequences of a cyber security incident. This should be analyzed in a *business impact analysis study*, which can be performed by a cyber security officer or consultant, which in turn is then integrated into a risk management plan by the CSO and other executives.

Human threats arise from both intentions and unintentional errors. Some sociologists have studied the field of human behavior to formulate ideas as to why people intentionally deceive other people and carry out malicious activities. A summary of these threats is provided in Table 1.

Threat	**Internal**	**External**
Current Employees	XX	
Contractors and Facility Managers	XX	
Customers/Clients		XX
Service Providers		XX
Former Employees		XX
Former Consultants		XX
Hackers		XX
Organized Crime Groups		XX
Terrorist Organizations		XX
Competitor Firms		XX
Social Action/Pressure Groups		XX
Rogue Nations		XX
Other (s)	XX	XX

Table 1. Summary of Human Threats to Cyber Security

Current employees may intentionally attempt to alter systems or steal data in retaliation for some type of work-related conflict. This situation may occur due to a missed promotion, low compensation structure, or workplace conflict. In fact, the most recent survey on cyber criminality indicated that most malevolent activities related to IT are actually perpetrated by insiders, with 70% of the organizations responding that they were aware that security breaches occurred in their organizations (Gordon, L., et al. 2006, CSI/FBI computer crime and security survey. Available online at http://www.gosci.com/2006survey.).

External threats evolve from former employees, contractors, and consultants, as well as various groups of *cyber warriors*. Hackers and organized crime rings are the most popular groups of outside threats that most cyber security officers consider.

Organized crime is another external threat to cyber security in the maritime sector. Through influence and pressure, these groups seek to take advantage of others in order to benefit themselves and their associates and sympathizers, profiting from such illegal activities as extortion, money laundering, drug sales, prostitution, and gambling. Today, they can also stalk people online, send threatening e-mail messages, and post messages on websites and blogs.

Terrorist organizations, rogue nations, and political/social action groups also pose threats to the critical infrastructures. Cyber terrorists normally fall into two categories: nationalists/extremists or foreign terrorists. The Internet is an attractive training ground, information dissemination tool, and group-think platform for these groups. No matter where they are physically resided, the Internet provides an inexpensive tool for destruction. In addition, rogue nations are classical enemies of a nation in both a traditional warfare context as well as from a cyber-warfare perspective. Finally, political and social action groups motivated by their own agenda also pose threats, some of which are physical threats.

In terms of the transportation infrastructure, a large denial of service attack could have devastating results. For instance, what would be the impact of a ship that explodes in a large port facility whereby emergency response systems are temporarily or permanently disabled? Today's government information systems store vast amounts of important information, and in the maritime industry some of these systems are available to the public at large, whereas others are accessible only to commercial companies that participate in selective government programs. There is also a wide variety of additional general business threats and risks that are also relevant to the maritime industry. Although they are common to other traditional organizations, it is worthwhile to acknowledge that these risks are also evident. They include sociological, criminal, political, economic, and legal issues (Alexander, Y. and Swetnam, M.S. Cyber terrorism and information warfare: Assessment of challenges, vol. 1. Dobbs Ferry, New York: Oceana Publications. 1999, p.38).

Ethical consideration in cyber security includes such issues as employee e-mail monitoring, acceptable use of policies, and disciplinary action plans that an organization must consider. Often, these are controversial issues in the workplace. For this reason, it is important to have a strict set of company policies including a corporate *code of conduct*.

2. Means of cyber actions

Information is a vital asset to every maritime organization. Any accidental or deliberate destruction or theft can cause damage to the company in a variety of ways. Depending on the criticality of the information, this could have dramatic effects on the organization.

Malware is a comprehensive term covering a variety of malicious forms of computer software. Included in this category are *computer viruses*, *worms*, and *Trojan horses*. Computer viruses are the most popular form of malware, and popular viruses have received a lot of discussion in the information systems field.

There have been a number of pervasive, powerful, and destructive computer viruses. Some of them have interesting names, such as ILOVEYOU, Melissa, Naked Wife, and WannaCry, which help make them appealing to the user when they appear as e-mail subject lines or file names. These viruses spread rapidly through the Internet due to the virus file being attached to e-mail messages. Computer viruses are not only common but also very costly in terms of their impact on business organizations. For instance, total costs of the ILOVEYOU virus were estimated to be $7 billion (Ghosh, A. K. Security and privacy for e-business. New York; John Wiley & Sons, Inc. 2001, p.87).

Denial of service attack is particularly important to web-based business. In essence a denial of service attack is overflowing of a computer system with more data than the system itself has the capacity to manage. This situation often forces system administrators to shut down their e-commerce systems and websites until the proper protection can be implemented.

Due to the diversity of network architectures, such as wide area, local area, virtual private, and various others, an organization needs to make various considerations. This is due to the underlying protocols being used. Two common risks in network security include sniffing and spoofing.

Sniffing involves an unknown party "listening" on the network using a hardware or software tool. This listening can involve undetected e-mail transmissions, free-text user ID and password details, and other valuable communications. A sniffer can be placed at a single location or in various locations within the company's network. This also makes the detection of such activities difficult for cyber security officers and network administrators.

Spoofing is also known as masquerading. In this attack, one user impersonates another user or pretends to be an external party such as a customer, vendor, or other third party. This type of attack can be easily complicating the cyber security enforcement and detection processes.

Organizations can implement various countermeasures to fight computer viruses. First, antivirus software should be installed on all PCs, file servers, and mail gateways. While it is critical to have this software loaded on workstations and servers, it is also important to make sure that this software is updated regularly. Second, companies should educate employees about the dangers of downloading software that has not been tested, approved, and licensed. For instance, shareware (i.e., software that is based on a liberal software distributed license) and freeware (e.g., software available without charge) can easily contain spyware and adware, which in turn can be used for computer zombies and botnets (Backhouse, J., et al. Risk management in cyberspace. In R. Mansell and B. S. Collins (Eds.), Trust and crime in information societies, Cheltenham, United Kingdom: Edward Algar Publishing. 2005, p.156).

3. Scope of the maritime cyber education at NVNA

Maritime University NVNA Varna has accredited specialties with developed curriculum in bachelor and master degree in the area of navigation, engineering, shipping and ports, maritime logistics, ICT, all of them civil and part of them - military oriented.

Specialties	Curriculum	
	Bachelor degree	Master degree
Navigation	XX	XX
Marine engineering	XX	XX
ICT in marine industry	XX	XX
Inland water navigation	XX	
Fleet and port management	XX	XX
Water transport management	XX	XX
Shipping	XX	XX
Ship electrical engineering	XX	XX
Ship repair	XX	XX
Ocean engineering	XX	
Marine safety and security		XX
Cyber security		XX
Logistic		XX

Table 2. Summary of NVNA curriculums

Scrutinizing all the curriculums, taking in mind the complexity of the information systems implemented in shipping and maritime business, and the promoted cyber security measures it could be summarized that:

- All the students are educated and trained to work their future jobs as users of information systems. The characteristics of seafarers and maritime business professions are to use a big amount of information that modern companies/infrastructures acquire, process, store and share using computers/consoles organized in local/global nets

- The cyber space domain is presented in curriculums as environment where the users benefit from connectivity, integrity and huge capacity
- The cyber security is not presented in bachelor's degrees
- There is no educational program for education of the students for the management security issues in the cyber area – for the positions 'Cyber Security Officer'
- The master program 'Cyber security' is oriented to educate students for the security issues in the cyber area – for the positions 'Cyber Security Engineer'
- The bachelor and master degree of the specialty 'ICT in marine industry' is dedicated to educate students for the positions: network engineers, systems administrators, application programmers, and system programmers
- There are no subjects in the bachelor and master programs that to support cyber security education of regular users of the information systems

Could be conclude that *the adapted at NVNA educational system is partly capable to prepare leaders, experts and users for the maritime cyber security domain*.

3. How to improve cyber awareness and cyber security in maritime domain by proper education and training

Based on the analysis of the identified threats and means of cyber attacks and existing curriculum in the NVNA the following suggestions for improving education and training for enhancing the cyber awareness and cyber security in maritime domain are elaborate:

- To establish curriculum for education of the students for the management security issues in the cyber area – for the positions 'Cyber Security Officer' – master degree program 'Management of cyber security'. The curriculum must bear two core fields – management and business courses (Information Technology Project Management; Security and Privacy of Information; Information Systems Legal Framework; Information Systems Strategy and others) and technical courses (Knowledge Management; Systems Integration; Systems Development; Incident Response Systems; Cybersecurity and others) (See: MBA in Information Systems, Georgia State University, http://www2.cis.gsu.edu/cis/program.mbasic.axp.).

- To introduce in the curriculum of all the specialties of the bachelor degree a subject 'Cyber security fundamentals' which can include:

= The key principles of cyber security: *Ease to Use, Need to Know, and Least Privilege* (Whitman, M. E. and Mattord, H. J. Principles of information security. Canada: Thompson Course Technology. 2005, p. 54).

= The primary objectives of the information technology security - *confidentiality, availability, integrity, nonrepudiation, and authentication*.

= The categories of information system cyber security - *physical controls* and *logical security* (Barber, R. The evolution of intrusion detection systems – the next step. Computers & Security 20 (2), 2001, p. 138).

= The organizational policies:

• Document classification schemes - supported by the organizational policies about how information and related documents can be shared within and outside the company. Information classification scheme with three major categories: *Public/Non Confidential*, *Secret/Proprietary, Top Secret/Highly Confidential* (Bosworth, S. and Kabay, M. E. Computer security handbook (4th ed.). New York: John Wiley & Sons, Inc. 2002, p.245).

• The company's culture on what types of information are allowed to be viewed and shared between various employee groups.

• Organization of security personnel in the company with a cyber security functions that can promote and enforce the company's cyber security policies and procedures. (Cyber systems and physical security department, chief cyber security officer*,* Cyber Security Officer, Cyber Security Engineers, network engineers, systems administrators, technicians, application programmers, and system programmers).

• Outsourcing some or all of organizational network management processes to a service provider to provide adequate information security.

= trusted user and his responsibilities.

Summary

The legal issues related to information and cyber security are diverse and often complex. For instance, global regulation of the Internet has often been cited as one of the major obstacles to further development of this important technology. Finally, we can expect that the field of cyber security will continue to expand and mature as information systems and communication technologies become more prevalent in the maritime and transportation industries.

Improving the cyber security in maritime domain is achievable through establishment of clear situational awareness having well-educated end experienced expert and managers in cyber security domain and basically informed 'trusted' regular information system users.

References

1. Alexander, Y. and Swetnam, M.S. Cyber terrorism and information warfare: Assessment of challenges, vol. 1. Dobbs Ferry, New York: Oceana Publications. 1999.

2. Backhouse, J., et al. Risk management in cyberspace. In R. Mansell and B. S. Collins (Eds.), Trust and crime in information societies, Cheltenham, United Kingdom: Edward Algar Publishing. 2005.

3. Barber, R. The evolution of intrusion detection systems – the next step. Computers & Security 20 (2), 132-145. 2001.

4. Bosworth, S. and Kabay, M. E. Computer security handbook (4th ed.). New York: john Wiley & Sons, Inc. 2002

5. Ghosh, A. K. Security and privacy for e-business. New York; John Wiley & Sons, Inc. 2001.

6. MBA in Information Systems, Georgia State University, http://www2.cis.gsu.edu/cis/program.mbasic.axp.

7. Whitman, M. E. and Mattord, H. J. Principles of information security. Canada: Thompson Course Technology. 2005.