https://doi.org/10.53656/ped2023-6s.08

Maritime Cybersecurity
Морска киберсигурност

MARITIME EDUCATION AND TRAINING (MET) CYBERSECURITY AND ISO/IEC 27001:2022 FROM MARITIME ACADEMY OF ASIA AND THE PACIFIC (MAAP) PERSPECTIVES AND TRADITIONS

VADM Eduardo Ma R Santos AFP (Ret.),
Engr. Gerardo D. Galang,
Michael A. Amon, MEM
Maritime Academy of Asia and the Pacific (Philippines)

Abstract. The International Maritime Organization (IMO) has promoted the cybersecurity or maritime cyber risk management in raising awareness across the industry on how to tackle the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures brought about by information or systems being hacked, breached, or compromised. Survey says that among all industries, the education sector ranked as the least secured with 87% having experienced at least one attack. Hence, Cybersecurity for MET is indispensable for the protection of networks, devices, and data from unauthorized or unintended access or illegal use. This paper shall be using quantitative and quantitative methods of research. Fortunately, ISO has published ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements and MAAP has its Cybersecurity Incident Response Plan. This paper shall use a historical research method related to MAAP Cybersecurity traditions and perspectives to align with the new international standard.

Keywords: maritime cybersecurity; maritime education

Introduction

Cybersecurity is important in maritime industry for it has a massive potential to affect the safety of the crew, ships, cargo and even ports. In shipping, cybersecurity is concerned with the protection of IT systems data, onboard ships hardware and sensors and data leak from unauthorized access, manipulation and disruption according to Marine Digital[2]. In our digital age, information security and data safety issues are critically important for even companies such as Twitter, Garmin, Intel and other huge industrial players, which were attacked in 2020. These cyberattacks happened also on-board ships and on-shore that includes IMO (2020), COSCO Shipping Lines (2018), Hurtigruten (2020), Iranian port (2020), Kennewick (2020), Barcelona port (2018), and Maersk (2017) to name a few.

In Education, account takeovers, ransomware attacks and personal information leaks are the prevalent school cyberattacks like the smishing attack on Deakin University at Australia with ten thousand leaks of current students and alumni and the Ryuk virus attack in Mexico crippling 24 schools in 2020 according to Hovhannisyan (Hovhannisyan 2023) of Forbes. The education sector, with an average of 2297 attacks against organizations every week, according to Check Point's *2022 Mid-Year Report,* garnered a 44% increase in cyber-attacks compared to 2021 according to Marcellino (Marcellino 2022). He added that most companies only have employees, schools have faculty and students making a much bigger network that is open and difficult to protect.

A glance at how big and wide the risk of cybersecurity breaches across industries that may result of a tantamount loss of billions or trillions of monies to sum all attacks shows that it is imperative for companies or organizations to address seriously and prioritize this issue. At a maritime higher education institution like MAAP, the process of identifying, analyzing, assessing and communicating a cyber-related risk needs to be established and taught to its staff and learners.

This paper shall be using quantitative and qualitative method of research to fully understand the Academy's cybersecurity perspective and traditions through the years, including innovations. Data shall be collected by survey and literature review to the sample primary source MAAP staff and learners.

The IMO's issuance of Guidelines on Maritime Cyber Risk Management on 7 June 2022; the Maritime Safety Committee adoption of Maritime Cyber Risk Management in Safety Management Systems (SMS) on 16 June 2017; ICS, IUMI, BIMCO[7], OCIMF, INTERTANKP, INTERCARGO, InterManager, WSC and SYBAss issuance of Guidelines on Cyber Security Onboard Ship V4; the International Association of Ports and Harbors' Ports Cyber Security Report; the International Association for Classification Societies (IACS) has issued a "Recommendation on Cyber Resilience (No. 166)"; the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements; and the United States National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity[6] are some of the sources that will reviewed in this paper that are critical to the maritime industry according to IMO[3].

This paper shall answer the questions “Are MAAP Cybersecurity perspective and tradition at par with the global management of maritime cyber risk?”, “How can ISO/IEC 27001 help MAAP to be more cybersecure in its operations”, and “What are the cyber risk controls that need to be established or enhanced covering protection, detection, contingency and response measures?”.

Review of Related Literature

Cyberattack

Intended to be a joke, the first known virus was loaded via floppy disk in 1982 by a 15-year-old high school student named Rich Skrenta according to Craig and Brooks (Craig & Brooks 2022). Inserted into an Apple II computer of a friend, the virus it attached to a game and designed to launch the 50th time the game was used. It just displayed a poem and the rest is history after it replicated as the virus resided into the computer’s memory.

On November 2, 1988, at around 8:30 pm, another student of Cornell University graduate school, Robert Tappan Morris, unleashed a maliciously clever program on the internet using a Massachusetts Institute of Technology (MIT) computer according to FBI. Known as the “Morris Worm”, as the first internet computer worm, the virus caused between $10 million and $100 million in damage repair cost according to Fortinet[4]. The “Morris Worm” struck in the year when the Internet was primarily the domain of academic researchers and infected computer systems at NASA, Stanford, Princeton, Johns Hopkins, Lawrence Livermore Labs, and UC Berkeley, among other institutions, according to Arctic Wolf[5].

This made me realize that the first major cyberattack was mostly on the education industry such as academic research, where MAAP is a part, and other industry. As I reflect on other readings, the cyber threats are more realistic in this age of digitalization and cybersecurity is a valuable necessity for an education organization. Let’s look deeper at how it all started on the literature available.

Rooting from where it all began shall give us better understanding of our paper. Before computer networks, Ruiz (2022) stated the first cyberattack was on a telecommunication network in France. Using a mechanical telegraph system, bankers Francois and Joseph Blanc took advantage of knowing advance market rising and falling as trading information. More than 100 messages were transmitted to the brothers up to 1836.

Table 1 below the shows the cybercrime according to Arctic Wolf[5] including the top 5 most notorious cyberattacks in history such as Robert Tappan Morris—The Morris Worm (1988), MafiaBoy (2000), Google China Attack (2009), A Teenager Hacks the US Defense Department and NASA (1999), and Hacking a Radio Phone System to Win a Porsche (1995).

Table 1. Cybercrime 1962 – 2022 by Arctic Wolf[5]

Year	Cybercrime	Year	Cybercrime
1962	Stealing passwords	2011	hackers stole information
1971	Creeper Virus	2013	spyware software, phishing attack, man-in-the-middle
1981	Morris Worm	2015	SamSam ransomware, spear-phishing attack
1994	Password sniffer	2016	TeleCrypt ransomware, spear-phishing
1995	Hacked into Citibank, Hacked large networks	2017	WannaCry Ransomware, posed as an Asian manufacturer
1998	Hacked U.S. government websites	2018	DDoS, cryptojacking
1999	Melissa Virus	2019	data breaches
2000	Mafiaboy	2020	Hacked personal data, data breaches
2005	Data leak	2021	Ransomware, Ransomware attack, zero-day
2008	combination SQL injection, password sniffers, and malware	2022	ransomware attack
2010	Stuxnet worm, Zeus Trojan, Operation Aurora		

According to Lukehart (2022), cybersecurity is a massive concern for colleges and universities heightened by offering hybrid or fully remote curricula. The top five cybersecurity threats facing the higher education are the following:

1. Phishing (spear phishing, whaling) – the hacker will pose as a trusted entity and exploit that trust to trick the user into providing sensitive information like passwords or even social security numbers.

2. Ransomware – type of malicious software that locates valuable data on a target system and holds it for a ransom sum.

3. SQL Injections – the hacker will enter a piece of malicious code into a query box on your website.

4. Data Breaches – malware or human error.

5. Outdated Technology - missing even one software update can make your organization more vulnerable.

Cybersecurity

Following the exponential attacks happening across all industries globally, we need to understand cybersecurity in simple terms as “The protection of software, hardware and data resources connected and stored on the internet” (Thakur & Pathan 2020).

Let’s look back at a memory as briefly surmised by Vikki Davies (Davies 2021), the cybersecurity key timelines. This protection was emphasized during 1970s as Bob Thomas’ Creeper worm virus moved over the ARPANET and Ray Tomlinson’s first anti-virus chased and deleted the Creeper. In 1987, competing claims by Andreas Lüning and Kai Figge for Atari ST and Ultimate Virus Killer, Czechoslovakians for NOD antivirus, and John McAfee for VirusScan as the innovator of the first commercial anti-virus product. As the world went online in the 1990s, firewalls and antivirus have been on mass production to protect the public.

In 2000s, the threats diversified and multiplied wherein information security has continued to advance in terms of standards and frameworks. ISO published in 2005 ISO/IEC 27001 as the world's standard for information security management systems (ISMS). The standard provided guidance for establishing, implementing, maintaining and continually improving an information security management system for companies of any size and from all sectors.

In February 12, 2014, the NIST of US developed a voluntary risk-based Cybersecurity Framework as a set of industry standards and best practices to help organizations manage cybersecurity risks. This framework consists of three parts such as the Framework Core (Functions (Identify, Protect, Detect, Respond, Recover), Categories, Subcategories, Informative References)), Framework Profile, and Framework Tiers (Tier 1: Partial, Tier 2, Risk Informed, Tier 3: Repeatable, Tier 4: Adaptive). This framework was updated to Version 1.1 last April 16, 2018 and revision is a work on progress with a draft hopefully submitted on March 31, 2023.

ICS, BIMCO, INTERTANKO and INTERTANKO submitted to IMO MSC on its 95th session about Industry guidelines on cyber security on board ship as measures to enhance maritime security last March 5, 2015. From four prime movers of the guidelines in 2021, there are nine producers and supporters of the guidelines on the Version 4 as stated in the introduction. The Guidelines on Cyber Security Onboard Ships include a cyber risk management approach comprising of the following:

- Identify threats.
- Identify vulnerabilities.
- Assess risk exposure.
- Develop protection and detection measures.
- Establish response plans.
- Respond to and recover from cyber security incidents.

On June 16, 2017, IMO’s Maritime Safety Committee adopted Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Other associations also issued guidelines such as Digital Container Shipping Association’s (DCSA) Implementation Guide for Cyber Security on Vessels v1.0, International Association for Classification Societies (IACS) has issued a "Recommendation on Cyber Resilience (No. 166)", and International Association of Ports and Harbors (IAPH) published IAPH Cybersecurity Guidelines for Ports and Port Facilities.

In Europe, the Institution of Engineering and Technology (IET) of London, United Kingdom in collaboration with the Department of Transport and Defense Science and Technology Laboratory published the Code of Practice Cyber Security for Ships in 2017 (Boyes & Isbell 2017). This code of practice strives to attain and maintain eight general security objective such as Confidentiality, Possession and/or Control, Integrity, Authenticity, Availability, Utility, Safety and Resilience.

The 2020s provided even greater challenge for cybersecurity professionals as it was the year of COVID-19, a health pandemic that spurred new threats, and the cybersecurity industry grew at the speed of light. According to Flynn (Flynn 2023), a multifaceted approach can minimize cyberattacks in higher education or any other industry. She enumerated some specific practical tips to consider concerning cybersecurity threats facing colleges and universities as follows:

1. Remain aware of changing trends.
2. Increase cybersecurity resources.
3. Educate people about the threats.
4. Consider reducing password usage.

In the Philippines, an initiative to formulate a National Cyber Security Plan (NCSP) 2005 forms part of the National Critical Infrastructure Protection Plan (NCIPP). Significant laws were enacted in 2012 on cybersecurity such the Data Privacy Act of 2012 and Cybercrime Prevention Act of 2012 (Sy 2016). In May 20, 2016 through Republic Act No. 10844 established the Department of Information and Communications Technology (DICT) in-charge of Philippine Cybersecurity Policy and Program Coordination. On May 2, 2017, DICT launched the NSCP 2022 with key strategic imperatives protection for critical infostructure, Government Networks, Business and supply chains, and individuals. The NCSP 2023-2028 is a target to be completed on May 30, 2023 (Balinbin 2022).

Part of the NCSO 2022 was cybersecurity awareness in various schools nationwide and integration of Cybersecurity and Academe by pioneering BS in Cybersecurity (AMA Computer University) and PSM in Cybersecurity (Holy Angel University). The Nautical Institute Foundation has developed a new online course, Maritime Cyber Awareness for Seafarers in partnership with HudsonCyber (Baskin 2022). Composed of three modules with videos and supplementary reading material, it is a three-hour self-pace course not taking place live. DICT Secretary Ivan John Uy stated on December 20, 2022 that short-term courses and long-term programs on cybersecurity will be launched in 2023 to help build the country's cybersecurity workforce in partnership with ISCO, Oracle, Intel, and Microsoft.

Discussions

MAAP Cybersecurity Perspectives and Traditions

The memorable and most devastating cyberattack the Academy experienced was caused by a worm virus that shut down a campus-wide network and computer infection. That triggered the cybersecurity awareness and acknowledgment of its importance to the organization's critical and day-to-day operations. This incident has breached the CIA triad framework/tenets of Cybersecurity that stands for Confidentiality, Integrity, and Availability, sometimes called AIC (Craig & Brooks 2022). This framework outlines the goals and objectives of a Cybersecurity program, such as:

- To makes sure that only authorized personnel are given access or permission to modify data (Confidentiality).
- To maintain the trustworthiness of data by having it in the correct state and immune to any improper modifications (Integrity).
- To ensure authorized users should be able to access data whenever required**.** (Availability).

On January 29, 2019, development of internet policy was instructed to MIITD Director Gerardo Galang and QMR to monitor and further elevated to Cybersecurity Policies and Guidelines during Management Review Board Meeting. The MAAP Cybersecurity Policy was approved two years later on April 19, 2021 as the pandemic hampered its full implementation.

With IMO adoption of resolution MSC.428(98) approving SMS with Maritime Cyber Risk Management, the Academy need to update our learners on cyber risk awareness onboard ships. The Innovation Project Office (IPO) has conducted webinars first to the graduating class on Cybersecurity on August 3, 2022 and had four sessions. The Risk Management in Maritime Cybersecurity (RMMCS) Group delivered the first webinar for 1Cl Cadets on August 03, 2022, via Zoom. This webinar was entitled, "Cyber Security, Threats, Actors, Motives, and Human Factor". Forty-two (42) Midshipmen attended the webinar. The discussed topics and the corresponding speakers are as follows:

- Maritime Cyber Security Terms and Definitions – Engr. Gerardo Ramon S. Galang.
- Human Element in Cyber Security – C/M Jeric E. Bacasdoon.
- Threat Actors' Motivations – Ms. Rosangela Anne D. Salaya.

The second seminar was facilitated and conducted by the project group last September 27, 2022, via face-to-face setup at the CAMS Auditorium with 75 First Class Cadets in attendance. The said seminar was entitled "Cyber Security in the Maritime Industry". Enumerated below are the topics that were discussed and their respective speakers:

- Introduction to Cyber Security in the Maritime Industry – Engr. Gerardo Ramon S. Galang.

- Cyber Security On-board Ships – C/M Jeric E. Bacasdoon.
- Cyber Security On-shore – Ms. Rosangela Anne D. Salaya.

The third seminar was held on March 27, 2023, at the Multipurpose Hall – Main Campus via face-to-face setup. A total of 73 1Cl Midshipmen participated in this seminar. The topic for this seminar was "Cyber Incident Response Plan", and the speakers were Engr. Gerardo Ramon S. Galang, Ms. Rosangela Anne D. Salaya, and C/M Jeric E. Bacasdoon.

For MAAP Staff, QAD and MIITD cascaded Cybersecurity Policy and Guidelines as integrated in Educational Quality Standard System (EQSS) Policy Manual and MIITD Manual on April 18, 2023. After a month, the HRD, QAD, and MIITD organized on May 24, 2022 an online Cybersecurity Awareness seminar for all which most of the participants found informative and relevant. A survey after the awareness seminar was conducted to capture the MAAP perspective on Cyber security with the following results on key aspects as shown Figure 1.

The data showed that 86.7% are using antivirus software, a high turnaround. Perhaps the remaining percentage may refer to their own devices that don't have licensed antivirus. All of the participants are using varied spyware and I believe most of them are bundled in antivirus software. With password protection practice of 64.63%, vulnerabilities such as using a default password/rarely changing password, saving password on web browser, and use of same passwords for different accounts are identified.

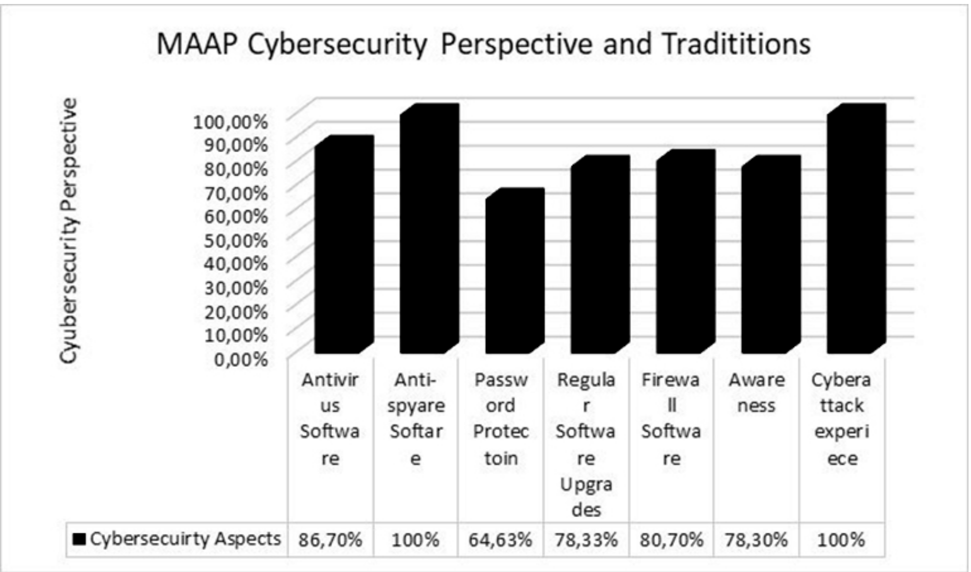

Figure 1. Cybersecurity Survey after Seminar

Regular software upgrade and awareness have almost the same 78% is which quite a high rate. 80.7% of Firewall is a good indicator for the level of intrusion protection. With the realization that 100% or all of the staff have experienced a cyberattack, it means it is imperative to be aware of cybersecurity and practice it.

A short discussion among IT personnel was conducted on May 29, 2023 to assess the controls that MAAP is currently implementing in terms of cybersecurity as follows:

- Policy and Plan – (MIITD Manual Annex II (MAAP Cybersecurity Policy), MAAP Cybersecurity Incident Response Plan (CIRP) (March 2, 2023)).
- Nine (9) Procedures and Guidelines – (Computer Virus Preventive Maintenance, Registration and Inspection of Handheld Devices, Corporate Email Account Procedure, Network Security Policy, Files, Systems and Databases Back-up Procedure, Information System & Corporate Accounts User Management Policy, MIITD Wi-Fi Procedure, LMS Technical Manual).
- Framework – NIST Framework used for the MAAP CIRP.
- Controls – 3-2-1 Backup Rule, Two-factor authentication for LMS.
- Infrastructure – Firewall (features: intrusion prevention, spyware protection, content filtering, app control, network support), Antivirus Software.

ISO/IEC 27001:2022

While there is a framework and guidelines for SMS and maritime industry, ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). This standard is a tool for risk management, cyber-resilience and operational excellence[1]. Jointly published by ISO and the International Electrotechnical Commission (IEC) under the responsibility of Subcommittee 27 (on Information Security, Cybersecurity and Privacy Protection) of ISO's and IEC's Joint Technical Committee on Information Technology (ISO/IEC JTC 1). ISO/IEC 27001 is widely used around the world for over 50,000 certificates were reported in more than 140 countries and by all economic sectors, ranging from agriculture through manufacturing to social services according to ISO Survey 2021.

On its third version, the former publication was in 2005 and 2013, it imbeds CIA triad principles by applying a risk management process and gives confidence to stakeholders that cyber risks are adequately addressed. According to ISO, the following are the benefits of implementing ISO/IEC 27001:2022:

- Reduce vulnerability to the growing threat of cyber-attacks.
- Be able to respond to evolving security risks.
- Ensure that assets such as financial statements, intellectual property, employee data and information entrusted by third parties remain undamaged, confidential, and available as needed.

- Provide a centrally managed framework that secures all information in one place.
- Prepare people, processes and technology throughout your organization to face technology-based risks and other threats.
- Secure information in all forms, including paper-based, cloud-based and digital data.
- Save money by increasing efficiency and reducing expenses for ineffective defense technology.

The 2022 version has 93 controls compared to 114 in the 2013 version, with four new control groups such as Organization controls (37 controls), People Controls (8 Controls), Physical Controls (14 controls), and Technology controls (34 controls). Additionally, there are eleven (11) new controls as shown in Figure 1.

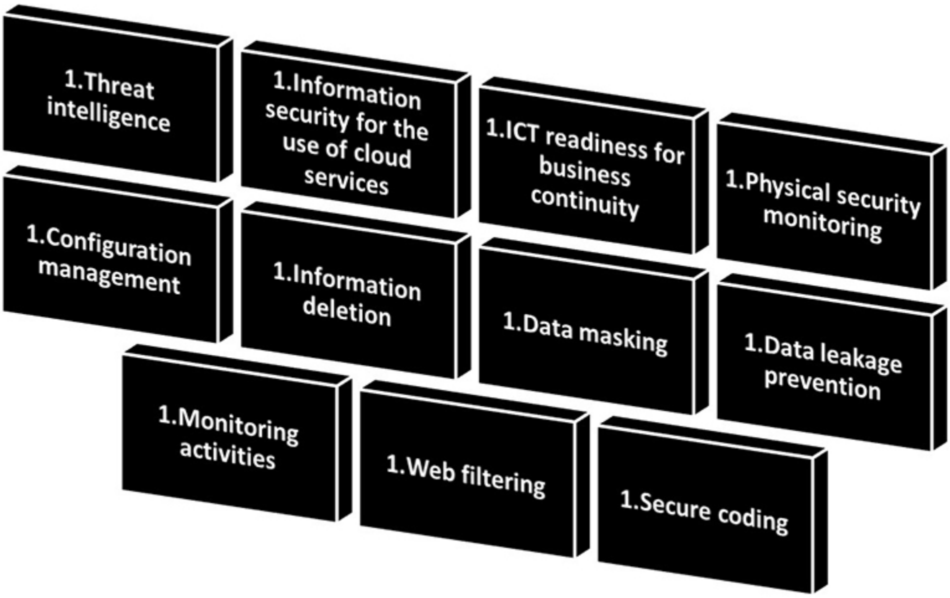
1.Threat intelligence
1.Information security for the use of cloud services
1.ICT readiness for business continuity
1.Physical security monitoring
1.Configuration management
1.Information deletion
1.Data masking
1.Data leakage prevention
1.Monitoring activities
1.Web filtering
1.Secure coding

Figure 2. ISO 27001:2022 New Controls

Furthermore, controls are made up of five types of attributes according to IT Governance Ltd. (2023) UK as follows:

- Cyber security concepts (identify, protect, detect, respond, recover).
- Information security properties (confidentiality, integrity, availability).
- Control type (preventive, detective, corrective).
- Operational capabilities (governance, asset management, etc.).
- Security domains (governance and ecosystem, protection, defense, resilience).

Cybersecurity in the Digital Era

The transition towards digitalization and automation in the maritime and education industry was hastened by the pandemic. Digital technologies and solutions (LMS, cloud simulation, smart classroom, online assessment, online information systems) are being used to increase competitiveness and enhance operational efficiency of schools. Onboard ships streams from sensors and other sources of information are used for decision-making and enhanced monitoring, control, quality assurance and verification. Data and information have gone digital in MET and vessel operation that needs to be protected via cybersecurity against current and futures threats and risks.

Conclusions and summary

MAAP cybersecurity has a strong framework/concept (NIST, CIA), infrastructure (firewall, antivirus, antispyware) and systems (policies, plan, procedures, guidelines) in place for cyber counter attacks. Awareness programs are started and need to be sustained to ensure manpower is equipped with the necessary knowledge and skills. Training of IT personnel and internal auditor to acquire critical skill sets in the cyber governance, protection, resilience is imperative.

With a number of maritime industry cyber security/risk management, guidelines, frameworks and laws on national and international level, MAAP should continue to educate and train learners (students, ratings, officers, stakeholders) in this imminent threat and reality.

A new international standard[1] (ISO/IEC 27001:2022) can be adopted by MAAP to enhance the existing MAAP Cybersecurity perspective (knowledge) and traditions (practice) to safeguard and protect the Academy's employees, assets, systems, network and program.

Recommendation

1. Implement Cybersecurity Awareness Program for newly hired employees and updates as part of MAAP standard induction system. This program includes possible cyber-attacks that the staff can encounter and advice to all on how to avoid, mitigate and recover using practical and technical MAAP cybersecurity guidelines, protocols, risk management and frameworks.

2. Training of IT personnel and internal auditors on cybersecurity like ISO/IEC 27001:2022 or another relevant course. The staff is to take ISO/IEC 27001:2022 foundation course with ten clauses requirements and ninety-three controls to help further MAAP cybersecurity using this standard. ISO/IEC 27001:2022 Internal Audit Course for auditor to ensure the international requirements are being implemented and applied throughout the Academy.

3. Development of Course for MAAP learners and other schools (mobility), three-hour modules for seafarers (self-paced) online or offline, or live

webinars series for other stakeholders. Instructors can teach the course to other schools if the cybersecurity course is internally, regulatory and statutory approved on each cybersecurity issue as they can be mobilized internationally. The modules for seafarers can start with the following topics as conducted in MAAP by IPO:

a. Cyber Security, Threats, Actors, Motives, and Human Factor.

b. Cyber Security in the Maritime Industry.

c. Cyber Security On-board Ships.

d. Cyber Security On-board Ships.

4. Use ISO/IEC 27001:2022 standard to enhance MAAP's cybersecurity perspective and traditions (policies, plan, procedures, guidelines, practice, framework, risk management) infrastructure and have certification as the need arises.

5. Conduct joint research or programs among IMLA members and/or maritime faculty to promote Cybersecurity awareness to maritime learners, faculty, seafarers, regulators and administrators. This research tends to elevate awareness to IMLA members and the institutes they belong to, creating IMLA member cybersecurity guidelines and frameworks.

NOTES

1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 21001:2018. Educational organizations - Management system for educational organizations – Requirements with guidance and use.
2. MARINE DIGITAL, 2023. The importance of cybersecurity in the maritime industry. Web site. Available from: https://marine-digital.com/article_importance_of_cybersecurity [Viewed 2023-05-17].
3. IMO, 2019. Maritime cyber risk. Available from: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. [Viewed 2023-05-17].
4. FORTINET, 2023. History of Cyber Warfare and the Top 5 Most Notorious Attacks. Web site. Available from: https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare. [Viewed 2023-05-17].
5. ARCTIC WOLF, 2023. A Brief History of Cybercrime. Web site. Available from: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. [Viewed 2023-05-18]
6. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018. Framework for Improving Critical Infrastructure Cybersecurity. Available from: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. [Viewed 2023-05-23].

7. BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC), 2021. The Guidelines on Cyber Security Onboard Ships Version 4. Available from: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf. [Viewed 2023-05-17].
8. BALINBIN, A. L., 2022. DICT crafts new cybersecurity plan to address more complex threats. Web site. Available from: https://www.bworldonline.com/technology/2022/12/15/493112/dict-crafts-new-cybersecurity-plan-to-address-more-complex-threats/. [Viewed 2023-05-23].
9. CRAIG, P. & BROOKS, C., 2022. *Practical Industrial Cybersecurity. 1st edn. Wiley*. Web site. Available from: https://www.perlego.com/book/3509338/practical-industrial-cybersecurity-ics-industry-40-and-iiot-pdf [Viewed 2023-5-12].
10. DAVIES, V., 2021. *The history of cybersecurity*. Web site. Available from: https://cybermagazine.com/cyber-security/history-cybersecurity. [Viewed 2023-5-22].
11. DELA CRUZ, R. C., 2022. *DICT to launch courses on cybersecurity to build PH capacity.* Web site. Available from: https://www.pna.gov.ph/articles/1191181. [Viewed 2023-05-23].
12. FLYNN, S., 2023. *Why Cyberattacks Hit Higher Ed and What You Can Do to Stop Them*. Web site. Available from: https://www.makeuseof.com/cyberattacks-hit-higher-education/. [Viewed 2023-5-23].
13. HOVHANNISYAN, G., 2023. *Cybersecurity Challenges In Education And How To Start Solving Them*. Web site. Available from: https://www.forbes.com/sites/forbestechcouncil/2023/04/07/cybersecurity-challenges-in-education-and-how-to-start-solving-them/?sh=11afc7d4f4ea. [Viewed 2023-5-17].
14. MASCELLINO, A., 2022. *Education Sector Experienced 44% Increase in Cyber-Attacks Over Last Year.* Web site. Available from: https://www.infosecurity-magazine.com/news/education-experienced-44-increase/. [Viewed 2023-05-17].
15. RUIZ, F., 2022. *What Was the First Cyberattack?* Web site. Available from: https://fluidattacks.com/blog/first-cyberattack/. [Viewed 2020-5-18].
16. LUKEHART, A., 2022. Top 5 Cybersecurity Threats Facing Higher Education. Web site. Available from: https://www.fierceeducation.com/technology/top-5-cybersecurity-threats-facing-higher-education. [Viewed 2023-5-23].
17. THAKUR, K. & PATHAN, A.-S. K., 2020. Cybersecurity Fundamentals. 1st edn. CRC Press. Available from: https://www.perlego.com/book/1522341/cybersecurity-fundamentals-a-realworld-perspective-pdf. [Viewed 2023-5-12].

REFERENCES

BOYES, H. & ISBELL, R., 2017. *Code of Practice Cyber Security for Ship*s. London: Institution of Engineering and Technology.

BASKIN, A., 2021. Cybersecurity and the human element. *Seaways The International Journal of the Nautical Institute,* pp. 12. ISSN 0144-1019.

🖂 **VADM Eduardo Ma R Santos AFP (Ret.), President**
Maritime Academy of Asia and the Pacific
Mariveles, Philippines
E-mail: emrsantos@maap.edu.ph

🖂 **Engr. Gerardo D. Galang**
Maritime Academy of Asia and the Pacific
Mariveles, Philippines
E-mail: gdgalang@maap.edu.ph

🖂 **Mr. Michael A. Amon**
ORCID iD: 0009-0005-0424-8403
Maritime Academy of Asia and the Pacific
Mariveles, Philippines
E-mail: maamon@maap.edu.ph