JOURNAL OF MARITIME RESEARCH

Vol XXI. No. II (2024) pp 278–284

ISSN: 1697-4840, www.jmr.unican.es

# Safeguarding Maritime Operations: A Proactive Approach to Maritime Cybersecurity

Anil Kumar Mishra[1,*], Dr. Shishir H. Mandalia[2], Mr. Harish C. Upadhyay[3]

*ARTICLE INFO*

***Article history:***
Received 17 Jan 2024;
in revised from 26 Jan 2023;
accepted 27 Mar 2024.

***Keywords:***
Maritime security; Cyber-threats; Disaster management; Cyber seaworthiness.

*ABSTRACT*

In the contemporary era of extensive digital connectivity, the marine sector assumes a pivotal role as a vital nexus for facilitating worldwide trade and commercial activities. Nevertheless, the industry's rising dependence on digital technologies has rendered it vulnerable to an escalating menace: cyberattacks. The aforementioned attacks possess the capacity to provide severe repercussions that exceed the ramifications of natural calamities. This article explores the imperative necessity for adopting a proactive stance towards marine cybersecurity, with a specific focus on the vulnerabilities introduced by human-induced catastrophes, including cyber-attacks. Case studies, such as the well-known Maersk disaster and cyberattacks targeting Operational Technology (OT) systems in Iran, highlight the vulnerabilities present within key marine infrastructure. The introduction of security ratings, such as Common Criteria, is regarded as a beneficial mechanism for evaluating and improving cybersecurity measures. Additionally, this research suggests adding a deterrent phase to current cybersecurity methods in order to effectively deal with risks before they happen.

## 1. Introduction.

The maritime industry, with its intricate web of global trade routes and supply chains, is a vital pillar of the world economy. However, the industry's increasing integration with digital technologies exposes it to new threats. This section provides an introduction to the paper, emphasizing the vulnerability of critical maritime infrastructure to cyber-attacks.

***"Man made disasters are more dangerous than natural disasters"***

The maritime industry, a cornerstone of global commerce and trade, is traversing uncharted waters in the digital era. The integration of advanced technologies and digital systems has revolutionized the industry, optimizing operations, enhancing efficiency, and ensuring timely deliveries across the world. However, this transformation has brought forth a burgeoning challenge-cyber threats. In an age where the virtual realm is as influential as the physical, the maritime sector stands exposed to an escalating threat landscape, where man-made disasters, particularly cyber-attacks, loom as menacing adversaries. The potential consequences of these attacks eclipse even those of natural disasters, rendering the need for a proactive approach to maritime cybersecurity more pressing than ever.

This article takes a look at the dangerous oceans of cyber threats, emphasizing how important it is to strengthen maritime cybersecurity to prevent hostile intrusions. We explore the physiology of cyberattacks, uncovering the complexities of their genesis and effects. We show the weaknesses inherent in vital maritime infrastructure by studying remarkable case studies like the disastrous Maersk incident and cyberattacks on Iran's Operational Technology (OT) systems. These case studies help us understand the severity of cyber threats and the necessity of enhancing our cybersecurity measures.

Cybersecurity guidelines have been developed by the Inter-

[1] Indian Maritime University. Mumbai Port Campus.

[2] Department of Library & Information Science, Sardar Patel University, Vallabh Vidyanagar, Gujarat.

[3] Indian Maritime University, Mumbai Port Campus.

[*] Corresponding author: Anil Kumar Mishra. E-mail: akmishra@imu.ac.in.

national Maritime Organization (IMO) and other industry parties. Nevertheless, the growing nature of cyberattacks calls for a paradigm shift in our approach. To achieve this, we suggest adding a proactive deterrence stage to the current cybersecurity techniques. Instilling a proactive ethos in the maritime cybersecurity landscape, this additional layer ***—Deter - Identify - Protect - Detect - Respond - Recover*** — prioritizes thwarting potential threats before they materialize.

In the subsequent sections, we explore the complexities of maritime cybersecurity by examining security ratings as a means of strengthening cyber resilience. Allowing consumers to make informed choices, we support the universal adoption of these ratings. Our goal, as we proceed on this path, is obvious:

- to strengthen the maritime domain against cyberattackers,
- to ensure safe operations and uninterrupted global trade in the era of digitalization.

## 2. The Growing Threat: Anatomy Of Cyber Attacks.

Cyberattacks have emerged as a significant threat in today's technologically advanced world, posing a significant danger to the maritime industry. To appreciate their potential impact on critical maritime infrastructure, it is essential to understand the anatomy of these cyberattacks.

Cyberattacks originate from the software implementation life cycle, which is a complex web of programs, data sets, and instructions that allow computers and digital devices to perform certain tasks. Software is vulnerable to cyberattack because it works differently than physical products. Software creation and use creates a digital landscape that has both risks and opportunities for exploitation. In essence, a wide range of applications, ranging from smartphones and personal computers to industrial equipment and spacecraft, are based on software.

***"We can rebuild homes destroyed by nature, but it's much harder to rebuild the trust and security shattered by man-made disasters."***

Let us compare a road construction project to understand software vulnerability. Like a road is made to connect two places, software is made to handle finance or IT applications. To ensure that the software accomplishes its intended task efficiently and correctly is the primary objective of a code developer. However, like roads with problems like landslides or theft-prone areas, software can have bugs or weaknesses that criminals can exploit. These vulnerabilities allow malware or viruses to get in and stop the software working.

The **End-User License Agreement (EULA)** is one of the most challenging elements when it comes to software. Software, unlike tangible products, often runs under licensing agreements, shifting user responsibility. Unlike consumer protections for tangible products, when a user installs software and accepts the terms of the EULA, they accept responsibility for any effects or risks associated with its use. This software feature highlights how important it is to understand and carefully consider the terms of software licenses before using it.

Cyberattacks start with the software implementation life cycle. Malicious actors exploit these shortcomings by breaking into software systems so that they cannot function properly. Data breaches and system malfunctions to full infrastructure control are some of the negative effects of this intrusion. Understanding this life cycle is crucial for understanding cyberattack anatomy, preparing us to strengthen our defenses, and navigating the complex maritime cybersecurity landscape.

## 3. Maritime Cyber-Security: Significant Cases.

***"Cyber attacks are the Nuclear Bombs of the new Era"***

### *3.1. Maersk – "NotPetya".*

The ransomware assault that occurred in 2017 targeting the company Maersk was a momentous incident with substantial and extensive consequences, impacting not only the organization itself but also exerting a profound influence on worldwide supply networks. In June 2017, Maersk, a prominent global shipping enterprise, experienced a cyberattack referred to as "NotPetya," which involved the deployment of ransomware. The malware successfully infiltrated and encrypted the entirety of the company's IT infrastructure, encompassing a substantial number of 50,000 computers and backup servers. The attack has significant global ramifications due to Maersk's handling of 20% of the world's shipping capacity. The global operations of ports, terminals, and logistics companies experienced significant disruptions due to their dependence on Maersk's systems for the purposes of coordination and tracking. The severity of the crisis was exemplified by the congestion in New Jersey, where an excess of 3,000 trucks were queued as a result of inadequate infrastructure to manage the influx of containers. According to reports, Maersk incurred an approximate financial loss of US$350 million as a result of the ransomware incident. This encompassed charges related to data and system recovery, operational losses, and company interruption. The Maersk disaster functioned as a catalyst for businesses spanning several industries, prompting them to become more alert and responsive. The incident brought attention to the susceptibilities of essential infrastructure to cyber assaults and emphasized the necessity for strong cybersecurity protocols.

### *3.2. Iran: Cyber-Attacks on OT systems- Cyber attacks can control the mechanical systems.*

The Stuxnet computer worm, which was detected in 2010, exhibited a high level of complexity and was designed with the explicit purpose of targeting supervisory control and data acquisition (SCADA) systems employed in industrial and operational technology (OT) settings. The perpetrators successfully penetrated the operational technology (OT) systems of the plant and assumed command over the centrifuges, resulting in their malfunction and subsequent self-destruction. Maritime enterprises heavily depend on a diverse array of operational technology (OT) systems to effectively oversee and regulate multiple facets of their activities, encompassing navigation, cargo management, engine control, and communication.

### 3.3. ECDIS.

Electronic Chart Display and Information Systems (ECDIS) serve a pivotal role as indispensable navigational aids employed on contemporary maritime vessels. The company offers up-to-date digital charts and navigation data in real-time to aid seafarers in navigating safely and efficiently. Cyber attackers may endeavor to compromise Electronic Chart Display and Information Systems (ECDIS) in order to modify navigational data. This can encompass modifying the ship's spatial coordinates or navigational information, so creating the illusion that the vessel is situated in an other geographic place or manipulating the intended trajectory of the ship.

### 3.4. Antwerp's cargo tracking system.

Cybersecurity measures were compromised by hacker collectives, purportedly affiliated with drug trafficking organizations, in their endeavor to infiltrate the cargo monitoring system at the Port of Antwerp. The vulnerability enabled unauthorized individuals to gain access to vital information, such as the precise whereabouts and security specifications of cargo containers. Consequently, these malevolent entities possess the capability to deploy vehicles with the purpose of intercepting containers before to their rightful owners. The penetration was executed using a two-pronged strategy, which encompassed the dissemination of malicious software to the personnel of the port and the utilization of key-logging devices, thereby facilitating remote entry into the port's cargo management systems.

## 4. Definition Maritime Cyber-Security.

Maritime cybersecurity refers to the implementation of measures aimed at safeguarding the Critical Information Infrastructure (CII) within the maritime sector. This pertains to safeguarding against cyberattacks and unintentional errors that possess the capability to incapacitate, disrupt, or commandeer the Information Technology (IT) and Operational Technology (OT) infrastructure within the maritime sector.

The essential infrastructures under consideration can be classified into three primary domains for analysis:

### 4.1. Systems in the general environment.

It refers to crucial systems utilized for navigation and communication in the maritime sector. Examples of such systems include Global Navigation Satellite Systems (GNSS) and Automatic Identification System (AIS).

### 4.2. Systems onboard ships.

It encompass critical components such as ballast systems and propulsion control, which play a vital role in ensuring the efficient functioning and safety of boats during their maritime operations.

### 4.3. Systems Ashore.

It refers to the monitoring and management of systems associated with cargo and port operations. These systems are crucial for ensuring the effective and secure operation of ports and maritime logistics.

The shipping insurance industry has introduced the term "***cyber seaworthiness***" to refer to the level of cybersecurity readiness for a marine vessel.

## 5. Anatomy Of The Cyber Attacks: How Its Carried Out.

### 5.1. Software implementation life cycle.

In order to ascertain the roots of cyber attacks, it is important to possess a foundational comprehension of the processes involved in software development and its subsequent commercialization. In contrast to tangible goods, software operates inside a discrete domain and adheres to certain marketing tactics. The unique characteristics of a system or network have a substantial impact on the emergence and development of cyber threats.

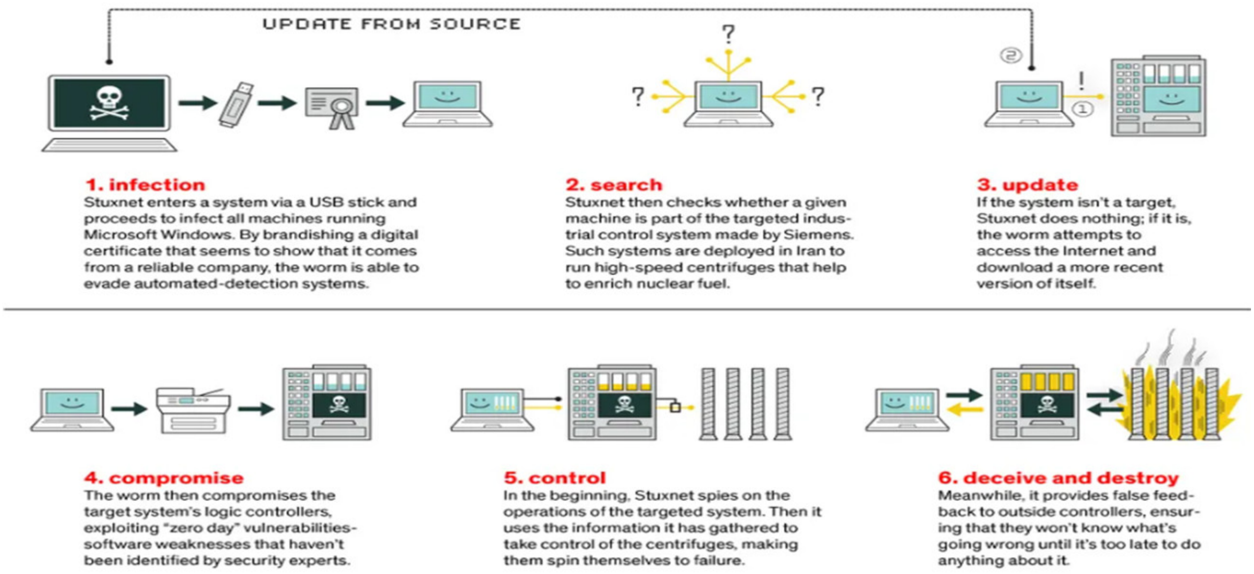
The phrase "Software" comprises a diverse array of programs, data sets, and instructions that enable computers and digital devices to perform specific tasks, functions, or operations. It serves as a crucial component in modern technology, acting as the foundation for a wide range of applications, including but not limited to smartphones, personal computers, industrial machinery, and spacecraft.

The utilization of an analogy that draws a parallel between software development and the construction of a road between Delhi and Mumbai seems to be an effective method for comprehending the underlying notion in a straightforward manner. Software is specifically engineered to do a specific activity or process. Similar to the construction of a road that serves as a means of connecting the cities of Delhi and Mumbai, software is developed with the purpose of accomplishing specific objectives, such as financial management, enterprise resource planning (ERP), and information technology (IT) applications. The primary objective of a code developer is to ensure the effective and accurate execution of software in accordance with its intended purpose, analogous to the goal of road builders in creating the most shortest and safest route between Delhi and Mumbai. The phrase "**and safest**" is intentionally crossed out because safety considerations are often given less priority in most software projects. Similar to how roads might face challenges such as landslides or places prone to theft, software systems can possess vulnerabilities or weaknesses that can be exploited by hostile actors, akin to thieves. These vulnerabilities serve as potential entry points for malicious software or viruses, which can then affect the normal functioning of the software.

### 5.2. Who is at Risk? The famous EULA.

When your car's airbags fail to deploy in a critical situation, you can typically hold the car manufacturer accountable through legal action. However, in the realm of software, the scenario is quite different. If a software system fails to withstand a

Figure 1: How Stuxnet worked.



**1. infection**
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

**2. search**
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

**3. update**
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

**4. compromise**
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

**5. control**
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

**6. deceive and destroy**
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

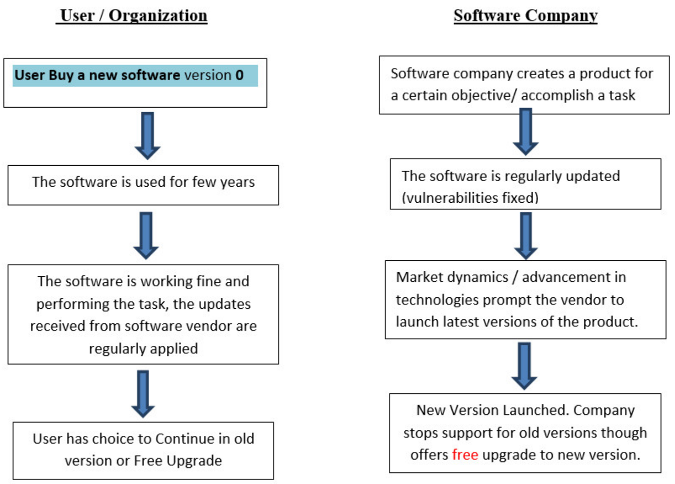
Source: L-Dopa.

cyber attack, the software company often disclaims any responsibility. This differs from the expectations we have with traditional physical products from vendors. With software products, the concept of ownership is often replaced by licensing agreements. These agreements, often outlined in the **End-User License Agreement (EULA)**, shift the burden of responsibility onto the user. In essence, when you install software and accept the terms of the EULA, you're acknowledging that you are responsible for any consequences or risks associated with the software's use.

In contrast to the consumer protections commonly associated with tangible products, the software industry tends to absolve itself of certain liabilities, making users bear a significant portion of the risks. This distinction underscores the importance of understanding and carefully considering the terms of software licenses before use, as they can significantly impact your rights and responsibilities as a user.

The **life cycle of a software** from a user and company perspective looks as below:

Figure 2: The Life-cycle of a Software.



User / Organization

User Buy a new software version 0

The software is used for few years

The software is working fine and performing the task, the updates received from software vendor are regularly applied

User has choice to Continue in old version or Free Upgrade

Software Company

Software company creates a product for a certain objective/ accomplish a task

The software is regularly updated (vulnerabilities fixed)

Market dynamics / advancement in technologies prompt the vendor to launch latest versions of the product.

New Version Launched. Company stops support for old versions though offers free upgrade to new version.

Source: Authors.

### 5.3. *Upgrades.*

Software companies often provide what they call ”free” upgrades for their products. However, it's crucial to recognize that these upgrades can come with substantial hidden costs. Take, for example, the transition from Windows 7 to Windows 11. While the upgrade itself may not incur a direct financial charge, it can necessitate significant collateral expenses.

***For instance***, upgrading from Windows 7 to Windows 11 may demand hardware enhancements, such as increasing the system's RAM from 1GB to 4GB. This is just one component; there are numerous other hardware and software changes that organizations may need to implement to ensure compatibility and optimal performance. These costs can run into millions for each upgrade cycle.

The recent cyber security incident involving Maersk serves as a stark reminder of the importance of comprehensive upgrades. Although major city systems were successfully upgraded and patched, the oversight of smaller city systems proved to be the weak link in their cyber security chain. This oversight allowed the attack to gain a foothold where defenses were less robust, highlighting the adage that

***"a chain is only as strong as its weakest link."***

In summary, the apparent "free" nature of software upgrades can mask substantial indirect costs, and neglecting to upgrade all components of a system can expose organizations to vulnerabilities, underscoring the critical importance of thorough and consistent upgrades.

## 6. Present Guidance and Standards on Cyber Security.

The International Maritime Organization (IMO) has taken decisive steps in order to solve and control maritime cyber risks. Actually, Maritime Safety Committee (MSC) and The Facilitation Committee (FAL) have issued "Guidelines on maritime cyber risk management" (MSC-FAL.1/Circ.3) as an answer to the increased number of cyber-attacks. The Guidelines completely accept NIST framework with five key elements: identification, protection, detection, response, and recovery (International Maritime Organization, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3, 2017).

- IMO has issued MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management.
- The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems.
- Guidelines on Cyber Security on board Ships issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.
- Consolidated IACS Recommendation on cyber resilience (Rec 166).
- ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cyber security (the NIST Framework).
- IAPH Cyber security Guidelines for Ports and Port Facilities

### 6.1. Analysis of the guidelines.

The IMO (International Maritime Organization) guidelines emphasize the importance of "Cyber Risk Management." This phase involves the systematic identification and management of cyber risks within maritime operations. Additionally, it stresses the need for maintaining a disciplined approach to cyber security, with principles that guide the handling of cyber risks. These principles typically include

***Identify - Protect - Detect - Respond – Recover***

The guidelines and standards outlined for combating cyber risks in the maritime industry are undeniably valuable and provide essential documentation. However, it's crucial to recognize that the field of IT and computing is constantly evolving, and shipping companies primarily focus on their core operations, not IT.

Addressing cyber risks effectively demands the involvement of dedicated and qualified IT professionals who possess the expertise to comprehend the intricacies of these risks. Software documentation, often spanning volumes of pages, can be complex, and some aspects require a seasoned eye to discern vulnerabilities that might not be evident at first glance.

In essence, while these guidelines provide a solid foundation, they underscore the need for specialized IT professionals who can navigate the nuances of cyber security, particularly in industries where IT is not the primary focus. These experts play a critical role in safeguarding against evolving cyber threats and ensuring the secure operation of digital systems in the maritime sector.

### 6.2. What is missing in the present guidelines.

The current guidelines primarily concentrate on mitigating cyber threats after they have already occurred. These guidelines assume that such risks are almost inevitable; outlining the actions organizations should take once a threat materializes. However, this paper suggests enhancing the existing methodology by introducing an additional layer of "**Deterrence**" to the cybersecurity framework, creating a more comprehensive approach:

**Deter - Identify - Protect - Detect - Respond - Recover**

- **Deter:** This new initial phase focuses on proactively deterring cyber threats before they even emerge. It involves implementing strategies and measures to discourage potential attackers from targeting the organization's systems and assets.

Putting the focus on the first layer i.e. deterrence will save the organization from cost and efforts required on the remaining layers.

Holy Gita chapter says that in order to control the mind it is important to make a screen to filter the thoughts , because once they enter the mind , it will take all the resources to manage it.

## 7. Concept Of Security Ratings of Softwares and Devices.

The concept of security ratings of the software's and devices is taking prominence in mission critical software's. There is need to implement the same to Maritime industry to minimize the risks and deter the cyber attacks.

The Common Criteria for Information Technology Security Evaluation, often referred to as **Common Criteria** or CC, is an internationally recognized standard (ISO/IEC 15408) for certifying the security of computer systems. It serves as a framework that allows users of computer systems to define their security requirements, both in terms of functionality (Security Functional Requirements or SFRs) and assurance (Security Assurance Requirements or SARs), within a document called a Security Target (ST). These requirements can also be drawn from Protection Profiles (PPs).

Vendors of computer security products can then use these Security Targets to demonstrate and make claims about the security features and capabilities of their products. Independent testing laboratories can assess these products to verify whether they indeed meet the security claims made by the vendors.

In essence, the Common Criteria establishes a structured and standardized approach to ensure that the process of specifying, implementing, and evaluating the security of a computer system or product is carried out rigorously and consistently. This evaluation is conducted at a level that aligns with the intended environment in which the product will be used.

Common Criteria maintains a registry of certified products, which includes a wide range of offerings such as operating systems, access control systems, databases, and key management systems. This certification process helps organizations make informed decisions about the security of the products they acquire, promoting trust and confidence in the cyber security landscape.

The **Evaluation Assurance Level (EAL)**, ranging from - EAL1 to EAL7, is a numeric grade assigned after completing a security evaluation based on the Common Criteria international standard, established since 1999. These increasing levels of assurance represent additional requirements that must be met to attain Common Criteria certification. The purpose of higher EALs is to provide greater confidence that the system's core security features are implemented reliably. It's important to note that the EAL level doesn't measure the inherent security of the system itself; rather, it indicates the level at which the system was tested and evaluated.

To achieve a specific EAL, a computer system must satisfy particular assurance requirements. These requirements predominantly involve aspects like design documentation, design analysis, functional testing, and sometimes penetration testing. Higher EALs demand more extensive documentation, analysis, and testing compared to lower ones. Achieving a higher EAL certification generally involves greater costs and time investments compared to achieving a lower EAL. The EAL number assigned to a certified system signifies that the system has successfully fulfilled all requirements associated with that specific level. In essence, it serves as a way to communicate the depth and rigor of the evaluation process for a given IT product or system's security features.

## Conclusions.

Organizations can indeed enhance their cyber security strategies by incorporating a deterrence layer. This additional layer emphasizes proactive measures to discourage cyber threats. Here are some key points related to this approach:

- **Security Ratings:** Universal efforts to encourage software companies to adopt security ratings are essential. These ratings can provide customers with valuable information about a product's security posture. By making security ratings a standard practice, organizations can more effectively evaluate and compare software products.
- **Customer Awareness:** Raising awareness among customers about the importance of selecting products based on security ratings is crucial. Educating customers about the risks associated with low-security-rated products can help them make informed decisions and prioritize security in their purchasing choices.
- **Risk Evaluation:** Organizations should weigh the pros and cons of purchasing products with low security ratings. While such products may be more cost-effective initially, they can pose significant risks and potential long-term costs in terms of data breaches, downtime, and remediation. Assessing these risks is vital.
- **Consequences Acceptance:** Accepting the consequences of choosing products with low security ratings means acknowledging the potential vulnerabilities and being prepared to deal with the aftermath. This may include investing in additional security measures, monitoring, and incident response capabilities.

Incorporating deterrence strategies, advocating for security ratings, and fostering customer awareness can collectively contribute to a more proactive and resilient cyber security landscape. It empowers organizations to make informed decisions that prioritize security and reduce the overall risk of cyber threats and incidents.

## References.

D. Kushner, The Real Story of Stuxnet, IEEE Spectrum 53, No. 3, 48 (2013). Available from https://spectrum.ieee.org/the-real-story-of-stuxnet [Accessed on $3^{rd}$ November, 2023].

Hopcraft, R. ., Tam, K., Dorje Palbar Misas, J., Moara-Nkwe, K., & Jones, K. (2023). Developing a maritime cyber safety culture: Improving safety of operations. *Maritime Technology and Research,* 5(1), 258750. Doi: 10.33175/mtr.2023.258750.

International Maritime Organization. (2022). Guidelines on Maritime Cyber Risk Management. IMO Publication. Available from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx [Accessed on $8^{th}$ November, 2023]

Karamperidis, S.; Kapalidis, C.; Watson, T. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. J. Mar. Sci. Eng. 2021, 9, 1323. Doi:10.3-390/jmse9121323.

Mraković I, Vojinović R. Maritime cyber security analysis – How to reduce threats? Trans Marit Sci. 2019;8(1):132-139. doi:10.7225/toms.v08.n01.013.

Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk, Capano, Daniel E. 2021. Available from https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ [Accessed on $3^{rd}$ November, 2023].