Designation: F3286 – 17

An American National Standard

Standard Guide for Cybersecurity and Cyberattack Mitigation[1]

This standard is issued under the fixed designation F3286; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide addresses the company or government organizational need to mitigate the likelihood of cyberattacks and reduce the extent of potential cyberattacks, which can leave sensitive personal data, corporate information, and critical infrastructure vulnerable to attackers.

1.2 These recommendations are meant to serve as a guideline for corporate and government organizations to adopt for the protection of sensitive personal information and corporate data against hackers.

1.3 Cybersecurity and cyberattacks are not limited to the maritime industry. With greater advancement in computer and information technology (IT), cyberattacks have increased in frequency and intensity over the past decade. These advancements provide hackers with more significant tools to attack vulnerable data and communication infrastructures. Cyberattacks have become an international issue to all governments and companies that interact with each other.

1.4 Cybersecurity and the safety of cyber-enabled systems are among the most prevailing issues concerning the maritime industry as well as the global economy. Cyberattacks could affect the flow of trade or goods, but operator errors in complex, automated systems may also cause disruptions that may be mitigated with proper policies and personnel training.

1.5 This guide is meant to provide strategies for protecting sensitive data onboard vessels and offshore operations.

1.6 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.7 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *Federal Standards:*[2]

46 CFR 140.910 Equipment

3. Terminology

3.1 *Definitions:*

3.1.1 *access control, n*—practice of selective limiting of the ability and means to communicate with or otherwise interact with a system, use system resources to handle information, gain knowledge of the information the system contains, or control system components and functions.

3.1.2 *application programming interface, API, n*—set of routines, protocols, and tools for building software and applications.

3.1.3 *botnet, n*—number of internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control or by passing messages to one another.

3.1.4 *capability, n*—ability to execute a specified course of action.

3.1.5 *communications, n*—means for a vessel to communicate with another ship or an onshore facility.

3.1.6 *compression, n*—reduction in the number of bits needed to store or transmit data.

3.1.7 *cybersafety, n*—guidelines and standards for computerized, automated, and autonomous systems that ensure those systems are designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors, especially in those areas of operation or maintenance that can affect human, system, enterprise, or environmental safety.

3.1.8 *cybersecurity, n*—activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and defended against damage, unauthorized use or modification, or exploitation.

[1] This guide is under the jurisdiction of ASTM Committee F25 on Ships and Marine Technology and is the direct responsibility of Subcommittee F25.05 on Computer Applications.

Current edition approved Dec. 1, 2017. Published January 2018. DOI: 10.1520/F3286-17.

[2] Available from U.S. Government Printing Office, Superintendent of Documents, 732 N. Capitol St., NW, Washington, DC 20401-0001, http://www.access.gpo.gov.

3.1.9 *data assurance, n*—perception or an assessment of data's fitness and integrity to serve its purpose in a given context.

3.1.10 *data, n*—quantities, characters, or symbols on which operations are performed by a computer being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

3.1.11 *detection processes, n*—methods of detecting intrusions into computers and networks.

3.1.12 *encryption, n*—conversion of electronic data into another form called ciphertext, which cannot be easily understood by anyone except authorized parties.

3.1.13 *exposure, n*—measure of a system at risk that is available for inadvertent or malicious access.

3.1.14 *firewall, n*—logical or physical break designed to prevent unauthorized access to information technology (IT) infrastructure and information.

3.1.15 *file transfer protocol, FTP, n*—standard network protocol used to transfer computer files between a client and server on a computer network.

3.1.16 *flaw, n*—unintended opening or access point in any software.

3.1.17 *human system, n*—interaction and contact between a human user and a computer system.

3.1.18 *hypertext transfer protocol, HTTP, n*—primary technology protocol on the web that allows linking and browsing.

3.1.19 *hypertext transfer protocol over secure socket layer, HTTPS, n*—protocol to transfer to encrypted data over the web.

3.1.20 *information technology, IT, n*—equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

3.1.21 *internet of things, IoT, n*—internetworking of physical devices, such as vessels, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

3.1.22 *information security management system, ISMS, n*—set of policies with information security management or IT-related risks.

3.1.23 *local area network, LAN, n*—computer network that interconnects computers within a particular area and does not connect to the internet; this applies to onboard ship networks.

3.1.24 *machinery control systems, MCS, n*—IT systems that report operating parameters or control operation of equipment, which commonly use programmable logic controllers (for example, fuel tank level indicators or throttle control systems).

3.1.25 *network, n*—infrastructure that allows computers to exchange data by wireless or cable wireless network interactions.

3.1.26 *operational technology, OT, n*—information system used to control industrial processes such as manufacturing, product handling, production, and distribution.

3.1.26.1 *Discussion*—Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

3.1.27 *original equipment manufacturer, OEM, n*—company that makes parts or subsystems that are used in another company's end product.

3.1.28 *phishing, v*—sending e-mails to a large number of potential targets asking for particular pieces of sensitive or confidential information.

3.1.28.1 *Discussion*—Such an e-mail may also request that an individual visits a fake website using a hyperlink included in the e-mail.

3.1.29 *programmable logic controller, PLC, n*—digital computer used for automation of industrial electromechanical processes.

3.1.30 *ransomware, n*—malware that encrypts data on systems until the distributor decrypts the information.

3.1.31 *remote desktop protocol, RDP, n*—proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection.

3.1.32 *resilience, n*—characteristics that enable a system to resist disruption and adapt to minimize the impact of disruptions.

3.1.33 *risk, n*—potential or threat of undesired consequences occurring to personnel, assets, or the environment as a result of vulnerabilities in systems, staff, or assets.

3.1.34 *risk assessment, n*—process that collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.

3.1.35 *risk management, n*—process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

3.1.36 *router, n*—device that forwards data from one network to another network regardless of physical location.

3.1.37 *scanning, v*—procedure for identifying active hosts or potential points of exploit or both on a network, either for the purpose of attacking them or network security assessment.

3.1.38 *sensitive information, n*—any digital data that can be classified as private or corporate not meant for public access.

3.1.39 *social engineering, n*—nontechnical technique used by potential cyberattackers to manipulate insider individuals into breaking security procedures, typically, but not exclusively, through interaction via social media.

3.1.40 *social media, n*—computer-mediated online tools that allow people, companies, and other organizations, including nonprofit organizations and governments, to create, share, or exchange information, career interests, ideas, and pictures/videos in virtual communities and networks.

3.1.41 *software, n*—intellectual creation that represents the real world as data and uses logic, that, when translated into electronically readable code and run on a computer, processes the data, allowing the requirements placed on the software to be realized in the real world.

3.1.42 *Subchapter M, n*—U.S. Coast Guard (USCG) regulations that legally define rules for the inspection, standards, and safety policies of towing vessels.

3.1.43 *transportation worker identification credential, TWIC, n*—provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA) and all USCG credentialed merchant mariners.

3.1.44 *water holing, v*—establishing a fake website or compromising a genuine site to exploit visitors.

3.1.45 *wide area network, WAN, n*—network that can cross regional, national, or international boundaries.

3.1.46 *wi-fi, n*—all short-range communications that use electromagnetic spectrum to send and receive information without wires.

4. Summary of Guide

4.1 The maritime industry is globalized. Shipping occurs across the world, transporting goods to different nations and continents. Technology integration onboard seagoing ships and vessels has increased the quality and reliability of communications, data recording, navigation, and record keeping. Wherever ships and marine craft go, there is a potential for cyber-enabled systems to impact ship operations and crew safety. At times, these impacts can emerge from human error or deliberate actions.

4.2 Commercial pressures and demands for efficiency and speed, as well as more control over shipboard systems, create the need for integrated systems that may be subject to misuse, abuse, or illicit access. Table 1 provides an overview of the motivation and impacts of a cyberattack.

4.3 Companies and governments that operate or own seagoing vessels should adopt measures and practices that will shape personnel and system access according to job requirements and need to know. For good practice, human and machine access to sensitive information should be kept to a minimum level. Access needs for third parties (for example, maintenance personnel, consultants, service engineers, and any non-crew personnel) should be addressed in company or government policies and procedures, or both.

4.4 Companies and governments may use cybersecurity training programs to educate the shoreside employees and mariners of the organization. Training programs and materials should provide useful tools and strategies to:

4.4.1 Reduce or prevent human errors in automated systems operations that could affect safety, correct system function, or ship data; and

4.4.2 Identify when a cybersecurity event occurs and how to stop or prevent one from happening.

4.5 Any implemented training program should apply to all members, shoreside employees, and mariners of a government or company operating seagoing vessels. Training programs should begin at the top of an organization and work through to the bottom thus following a hierarchical approach and response to cyber-system events and their impacts on the company, ship, or organization.

4.6 Training programs should focus on and follow a general procedure including the following steps:

4.6.1 Risk identification,

4.6.2 Risk detection,

4.6.3 Protection of personnel and vulnerable or critical infrastructure,

4.6.4 Mitigate effects of cyberattack,

4.6.5 Recover stolen or lost data, and

4.6.6 Restoration of systems to fully operational status.

4.7 Ship systems have become increasingly integrated with navigation, communications, recordkeeping, logistical data, corporate data, personal data, and ship-operating systems. These systems may be running on the same information infrastructure. With this interconnectedness comes complexities and interdependencies that can result in unexpected vulnerabilities. Even systems that use air gaps for security, such as machinery control systems, may be vulnerable to errors and attacks because of contamination with malware or malicious

TABLE 1 Impacts of Cyberattack[A]

Group	Motivation	Objective
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo
Opportunists	• The challenge	• Getting through cyber security defenses • Financial gain
States State-Sponsored Organizations Terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure

[A] Courtesy of BIMCO, Guidelines on Cyber Security Onboard Ships, February 2016.

code from diagnostic equipment. Vulnerabilities that present openings to outside connections can become weaknesses. So, it is vital for organizations to understand the origins of system vulnerabilities and likely means of attack.

4.8 As technology advances, IT systems require greater attention and resources to sustain and maintain them for continued operations and system reliability. Many older IT systems, especially in the maritime industry, use outdated technology that can endanger the confidentiality, integrity, and availability of data, therefore, creating previously undetected cyber risks and vulnerabilities.

4.9 In the United States, recent cybersecurity legislation passed by Congress and authorized by the President has begun to address the rapidly growing concerns for cybersecurity and points towards the development of new technologies for government agencies and private industry in the years ahead.

4.10 Governmental regulations, such as Subchapter M, 46 CFR 140.910, now permit and encourage the use of electronic records in addition to or in lieu of manual logging. The move to electronic recordkeeping and the sensitivity of the information these records contain impose new challenges to the secure access of the information, the sharing of the information with inspectors and auditors, the media to which this information is securely stored and backed up, and the methods required to access the information in a secure manner.

5. Significance and Use

5.1 To maintain the integrity of potentially vulnerable information systems while the vessel is at sea or in port, strategies and procedures can be used by every company, organization, and ship. Mitigating potential cyberattack events will allow for a better economic environment through secure consumer, employee, and corporate data. Informational infrastructure between ships, platforms, and onshore facilities are more interconnected today than a decade ago. The long-term health and economic viability of ship owners and operators depend on establishing and maintaining security that can measured and monitored.

5.2 With the increase in cyberattacks in recent decades, maritime-based companies and governments have cited a need to update and train their workforce to mitigate the loss of data or intellectual theft from onboard systems.

5.2.1 Vulnerable onboard systems can include, but are not limited to:

5.2.1.1 Cargo management systems;

5.2.1.2 Bridge systems;

5.2.1.3 Propulsion and machinery management and power control systems;

5.2.1.4 Access control systems;

5.2.1.5 Passenger servicing and management systems;

5.2.1.6 Passenger facing public networks;

5.2.1.7 Administrative and crew welfare systems;

5.2.1.8 Communications systems;

5.2.1.9 Distributed computing devices that support an internet of things (IoT)-enabled ship; and

5.2.1.10 Onboard sensors that facilitate wheelhouse automation, alerting, and IoT transmission.

5.2.2 Many of these systems are critical to mariners while at sea. If any of said systems failed or were compromised while at sea because of a cyberattack, then the ship and its security could be compromised.

5.3 By adopting these practices, mariners and shoreside employees at all levels of the organization should be able to identify potential threats or risk factors, as well as the abnormal indications that show a cyberattack underway.

5.4 Cyberattacks can occur in multiple forms including, but not limited to, the following practices:

5.4.1 Social engineering,

5.4.2 Phishing,

5.4.3 Waterholing,

5.4.4 Ransomware,

5.4.5 Scanning,

5.4.6 Spear-phishing,

5.4.7 Deploying botnets, and

5.4.8 Subverting the supply chain.

5.5 These suggested strategies extend to all individuals of a corporation, government, or organization. By adopting a basic and developed capability to defend from cyberattacks, mariners can continue proper practices out at sea while feeling confident that safety critical systems, business-critical data, personal data, and records are safe.

5.6 In the event of system error, or in the case of cyberattack or infection, any files required to rebuild or repair a personal computer (PC)-based onboard system shall be on the ship already rather than from off-board sources using satellite communications systems. Most vessels currently do not have operating system disks on board, let alone proprietary software, drivers, or patches. This connectivity constraint and lack of multiple failsafe outputs also provide a single point of failure and vulnerability. In the future, system software and firmware may be kept current with over-the-air updates, which shall be encrypted.

5.7 There are cross-system considerations that shall be considered for cyber-enabled ships. They may include such factors as:

5.7.1 Human-system interfaces;

5.7.2 Software availability, versions, and licensing;

5.7.3 Network and communications, including remote access methods;

5.7.4 Data trustworthiness and availability (that is, data assurance);

5.7.5 Diagnostic and evaluation equipment that may be required to diagnose system problems;

5.7.6 Cybersecurity, especially as it applies to safety critical and ship critical systems; and

5.7.7 Onboard sensors and IoT infrastructure that provide data for ship operations and command decisions.

5.8 By adopting these practices, companies and governments will notice the benefits of better cybersecurity. Some benefits may include, but are not limited to:

5.8.1 Better business performance;

5.8.2 Increased bandwidth efficiency provided by modern satellite communications;