2023-01-24

Raising the Standard of Maritime Voyage Data Recorder Security

Hopcraft, Rory

10.3390/jmse11020267
Journal of Marine Science and Engineering
MDPI

Journal of
Marine Science and Engineering

MDPI

Article

Raising the Standard of Maritime Voyage Data Recorder Security

Rory Hopcraft *, Avanthika Vineetha Harish, Kimberly Tam and Kevin Jones

CyberSHIP Lab, Faculty of Science and Engineering, University of Plymouth, Plymouth PL4 8AA, UK
* Correspondence: rory.hopcraft@plymouth.ac.uk

Abstract: Voyage Data Recorders (VDRs), often referred to as the 'black boxes' of the shipping industry, collect and store vital data from key sensors and locations around the ship. This data plays a pivotal role in incident investigation, as was seen in the grounding of the Costa Concordia in 2012, and the sinking of the El Faro in 2015. With such an important role to play, the International Maritime Organization (IMO) has mandated that all SOLAS registered ships carry a VDR, which can demonstrate compliance with internationally agreed standards. Without a VDR compliant with these standards a ship cannot sail. However, the rise in the number, and sophistication, of digital devices are making the sector increasingly vulnerable to cyber-attacks. This paper will demonstrate a number of high-risk VDR cyber security vulnerabilities and review the current international technical standards covering all VDR devices being manufactured and used today, drawing attention to the minimum security requirements. The paper will go on to discuss how these standards fail to promote the necessary levels of cyber security needed to protect VDRs from today's cyber risks, amidst increased demands for digital connectivity for remote and autonomous operations. The paper will conclude by proposing several amendments (technical and non-technical) to the current standards which, if adopted, will help increase the minimum level of security of VDRs. Industry opinions were gathered on this topic, and their beliefs have been included across this paper.

Keywords: maritime; cyber security; voyage data recorder; performance standards

Citation: Hopcraft, R.; Harish, A.V.; Tam, K.; Jones, K; Raising the Standard of Maritime Voyage Data Recorder Security. *J. Mar. Sci. Eng.* **2023**, *11*, 267. https://doi.org/10.3390/jmse11020267

Academic Editor: Mihalis Golias

Received: 29 November 2022
Revised: 13 January 2023
Accepted: 17 January 2023
Published: 24 January 2023

1. Introduction

During any incident investigation, it is vital to have access to accurate information pertaining to the incident, as this can provide tangible proof of the cause or causes. For this reason, Voyage Data Recorders (VDRs) record detailed information from various sources around the ship [1]. The purpose of the VDR is to store data in a secure and retrievable form for at least 30 days (720 hours) and 48 hours on the long-term and the fixed/float-free recording mediums respectively. This data includes information concerning the date and time, ship's position, speed heading, rudder and engine orders, bridge and communications audio and specific equipment data like radar captures and Automatic Identification Systems (AIS) information (for the full list see [2,3]).

The inclusion of the VDR as part of a ship's systems came about after a number of serious maritime incidents in the 1980's and 1990's [4]. This includes one of the most notable incidences, the sinking of the MS Estonia with 852 people dead [5]. Entering into force in 2000, the International Maritime Organization's (IMO) Maritime Safety Committee (MSC) outlined the requirements for ships to carry VDRs as a way to understand the root cause(s) of maritime accidents. Thus, this data is used during maritime accident investigations by authorities like the UK's Maritime Accident Investigation Branch (MAIB) to help ensure these incidents do not reoccur [6].

Several high-profile cases have relied on the data VDRs had recorded in the critical moments leading up to a catastrophic incident. Prime examples of this are the grounding of the Costa Concordia in 2012 and the sinking of the El Faro in 2015. In both these high-profile

cases, investigators went to significant lengths to retrieve the ship's VDRs to understand the key factors surrounding the incidents [7–9]. As a critical part of incident investigations, the manipulation or outright disappearance of VDR data can lead to investigation dead ends. What is more, as [10] argues, cyber attacks are becoming more prevalent and accurate data about systems becomes increasingly important in understanding what happened.

In a data driven world it is not surprising that organisations want to gather information about vessels, and their performance, to better understand how to make operations more efficient leading to potential cost savings. The traditional, and still current practice for this data collection is through the use of voyage report data, particular that data collected during the noon report. The noon report includes information about the amount of fuel or water remaining on board as well as environmental information like average wind direction and force. However, some VDR manufacturers are now offering services which use the VDR data outside of incidents as a way for companies to better understand their operations, and onboard actions, to help improve training or operational procedures [11]. So, as illustrated by [12] it is possible to utilise the data recorded by the VDR, alongside other sources like the noon, to better understand energy-efficient operational measures, for example sailing speed optimization.

Furthermore, the international community is continually moving towards securing their digital infrastructure, through the implementation of international regulations like the Network and Information Systems (NIS) Directive [13] and the European Union's (EU) General Data Protection Regulation (GDPR) [14]. Whilst hardware manufacturers and software developers are not operators of essential services, the NIS Directive argues that they have an important role to play in the EU's security stance. Therefore, they should be making efforts to improve the cyber security of their devices. Furthermore, the European Union Agency for Cybersecurity (ENISA), argue that inland, sea and coastal passenger and freight transport companies can be defined as essential services providers [15], and are then obligated to implement a minimum level of cyber security into their practices.

There could also be financial ramifications for the company if they fail to ensure the security of devices. Considering that one of the data sources of the VDR records are via microphones (some manufacturers now include video feed recording [16]) from around the ship, it is not unfeasible to imagine that personal conversations could be recorded. These conversations could contain personal data, and would therefore fall under the remit of the GDPR requirements. So, in the case of this data being stolen, it could lead to financial ramifications for the company [17]. Furthermore, as will be discussed later (Section 4.2), there are new compliance requirements being released by ship Classification Societies, which stipulate more stringent security measures. Non-compliance to those requirements could lead to a ship being deemed unfit to sail, which could cost the company in lost revenue and reputation damage.

To ensure our critique of current standards are based on ground truths, this paper tests the cyber security of real VDR equipment to underpin our recommendations. Whilst many of the technical requirements covering VDRs have been updated since their inception before the mass proliferation of the internet, this paper will argue that some requirements predate the current capabilities of malicious actors. One such requirement states that VDRs will typically have Universal Serial Bus (USB) ports for updating the system, as well as retrieving stored data. Like the VDR investigated in this paper, many of these devices remain isolated from the internet, meaning accessibility is limited to those with direct access to the ship, e.g., company employees like crew. However, as the Honeywell USB Threat Report shows, USBs are one of the top threat vectors to industries including shipping, with an increase from 37% in 2021 to 52% in 2022 [18]. Therefore, as argued by [19], a motivated insider could use their access, alongside a USB plugged into an open port on the VDR to manipulate its operation. There is an interesting possibility that crew members might alter or wipe evidence data to hide their mistakes. The use of a cheap USB device to hide incriminating evidence may be perceived to be better than paying huge consequences of being caught, including unemployment and imprisonment, particularly if they are from

a poorer social background. The risks to these devices are only set to increase as the sector moves towards remote monitoring and control. As such, many new VDRs offer the ability to both access and store data remotely. This paper will explore various different attacks primarily utilising the USB drive as an attack vector, and highlight how the technical, and performance standards currently, if implemented, do not provide sufficient protection against these attacks.

To demonstrate the importance of the VDR the International Maritime Organization (IMO), through the Safety of Life at Sea Convention (SOLAS), has mandated the carriage of VDRs on any SOLAS registered ship. Chapter 5, Regulation 20 of SOLAS obligates all passenger ships, roll-on roll-off (ro-ro) passenger ships and cargo ships over 3000 gross tonnage constructed after 2002 to carry a VDR [20]. For ships constructed before 2002, the IMO requires the carriage of an S-VDR (Simplified Voyage Data Recorder). The IMO, through the ratification of various resolutions such as MSC.163(68) for S-VDRs and MSC.333(90) for VDRs, has set about defining the performance requirements of these devices. However, it is the international standards organisations, like the International Electrotechnical Commission (IEC), that define the exact technical and performance requirements of these devices. To this end, there are several international standards that specifically cover ship's VDRs, for example, IEC 61996-2013+A1:2021—Maritime Navigation and Radio Communication Equipment and Systems—Shipborne Voyage Data Recorder .

This article will argue that the current standards, which represent the minimum level these devices must demonstrate, do not go far enough to cover the security risks these devices face today. This article provides a comprehensive review of the published IMO and IEC standards and the security-related requirements relevant to VDRs currently found on ships within the world fleet. Then the paper will demonstrate through a rigorous penetration test on an up-to-date VDR from a major manufacturer, that these systems have various vulnerabilities, which puts their ability to operate normally at risk. The paper will then discuss how the current security requirements are not stringent enough to protect VDRs and their data from both the simple and complex cyber-attacks demonstrated, before offering a selection of recommendations for improvements in the current standards. These recommendations, validated through discussions with industry experts as part of a maritime-specific symposium, consider both current, and future risks to VDRs, as well as the perceived financial and procedural burden for their implementation.

2. Current Technical Standards

Most VDRs consist of a core module, which acts as a data acquisition unit gathering information from sensors and bridge equipment and stores it on internal hard drives. VDRs also have two external storage mediums, one fixed and the other float-free. The final component of the VDR is the bridge interface, which is the Graphical User Interface (GUI) that allows the crew to monitor the status of the VDR. Figure 1 illustrates the basic architecture of a VDR.

The Core Unit of the VDR (as seen in Figure 2) normally consists of a standard interface for uploading/downloading data (USB), a dedicated computing device running the VDR software, and some form of input and output interface (Ethernet or serial) for receiving data from sensors and sending recordings to storage. The Core Unit also includes two hard drives that mirror each other, designed so that if one drive fails, the second one can be used. For simplicity, these storage drives have been labelled as "hard drives" in Figure 2. This figure also illustrates the required uninterruptible power supply, which mitigates the risk of a power outage affecting the VDR.

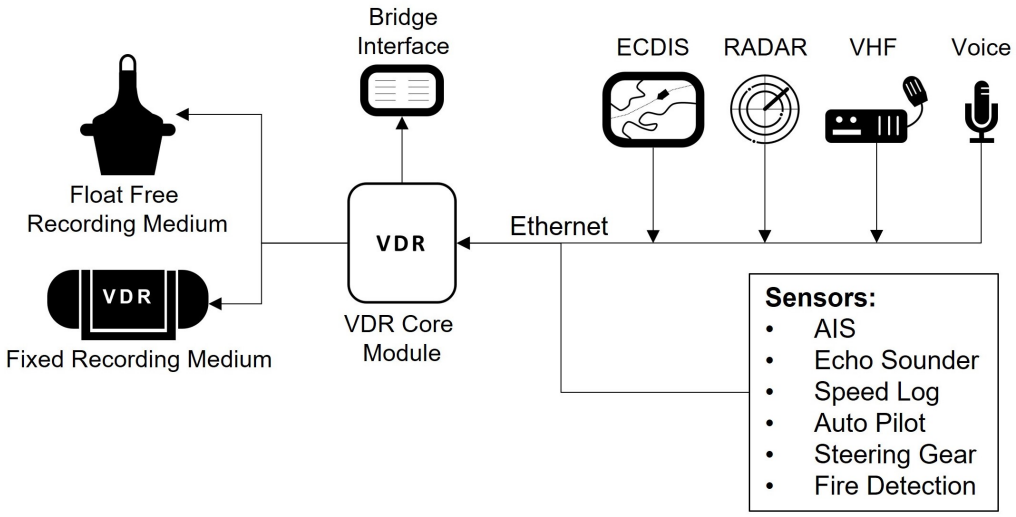

Figure 1. Basic VDR Architecture.

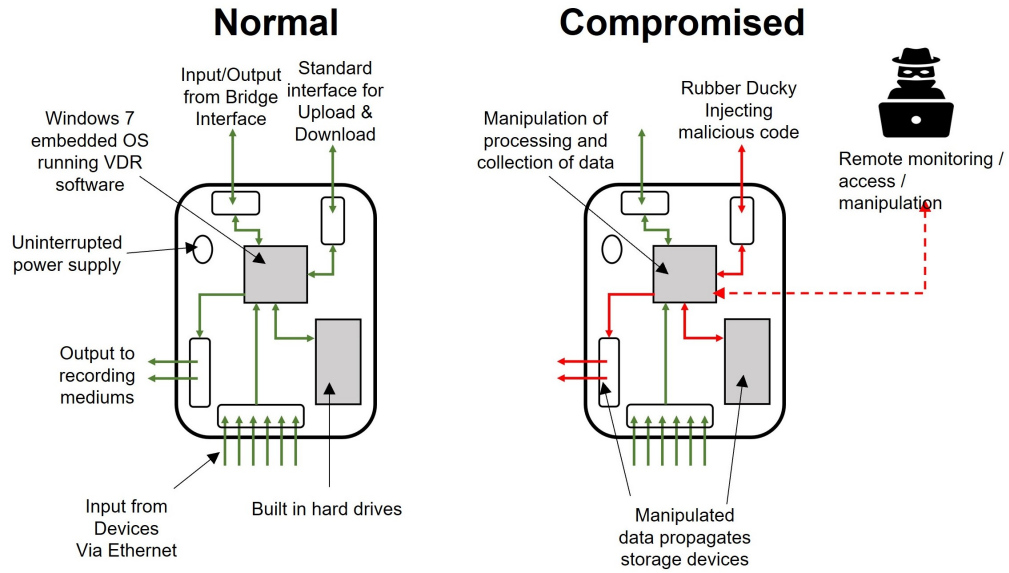

Figure 2. VDR Core Unit Components and Data Flows (normal and compromised operation).

Due to the importance, variety, volume, and complexity of VDR data, it is essential to protect each of these components against accidental or intentional damage. The IMO, through the use of resolutions, has outlined what it considers to be the minimum requirements these devices must demonstrate to ensure they fulfil their role within a ship's system. It is then through international standards set by the International Organization for Standardization (ISO) which outline the exact technical specifications that these devices adhere to. However, there is no definitive list of the exact standards these devices must demonstrate compliance with. Therefore, to focus this review, and to ensure all relevant standards were considered, the authors looked to a number major VDR manufacturers' VDR approval certificates, this list is not exhaustive of all VDR manufacturers. Table 1 summarises the standards each device is approved to.

Table 1. Summary of current Standards VDRs comply too [21–25].

Manufacturer Device	AMI Marine X2 VDR	Furuno VR-7000 VDR	NetWave Systems NW-6000 VDR	Danelec Marine DM100 VDR G2	Kelvin Hughes X-VDR
IMO Regulations	A.694(17) MSC.36(63) MSC.97(73) MSC.191(79) MSC.333(90)	A.694(17) MSC.163(78) MSC.191(79) MSC.302(87) MSC.333(90)	A.658(16) A.662(16) A.694(17) A.810(19) A.830(19) A.861(20) MSC.81(70) MSC.163(78) MSC.333(90)	A.694(17 MSC.36(63) MSC.97(73) MSC.191(79) MSC.302.(87) MSC.333(90)	A.694(17)) MSC.36(63) MSC.191(79) MSC.333(90)
IEC Standards	IEC 60945:2002 IEC 62288:2014 IEC 61996-1:2013 IEC 61162-1 IEC 61162-2 IEC 61162-450	IEC 61996-1:2014 IEC 61996-2-1 IEC 61162-1 IEC 61162-2 IEC 61162-450 IEC 60945:2002 IEC 62288 IEC61924-2	IEC 61996-1:2013 IEC 60068-2-27 IEC 60936-1:1999 IEC 60936-3 IEC 60945:2002 IEC 61097-2:2002 IEC 61097-7:1996 IEC 61162 IEC 61260 IEC 61672 IEC 61993-2 IEC 62288 IEC 61162-450	IEC 61996-1:2013 IEC 61996-2 IEC 60945:2002 IEC 61162-1 IEC 61162-2 IEC 61162-450 IEC 62288:2014 IEC 62923-1:2018	IEC 60945:2002 IEC 62288:2014 IEC 61996-1:2013 IEC 61162-1 IEC 61162-2 IEC 61162-450

As Table 1 highlights, there is a multitude of standards that VDRs can comply with. Some of these standards are generic standards like IEC 61672-1:2013—Electroacoustic—Sound level meters, whereas others are specific to VDRs, for example, IEC 61996-1:2013—Maritime navigation and radiocommunication equipment and systems. Shipborne voyage data recorder (VDR). As Table 1 illustrates, some devices, like the NetWave device, have approval to more standards than others. Therefore, for the research to focus on the minimum acceptable requirements of the VDR, this paper will focus on those requirements which th devices listed share compliance with. Furthermore, as this article prioritises the development of security requirements for devices moving forward, the review will focus on the current, and most up-to-date versions of these requirements. For the duration of this paper, the term security will imply both physical and digital/electronic security. It is important to note that the off-the-shelf device (VDR_T) used for our experimentation (see Section 3) was from a major manufacturer, and complied with all the relevant standards listed.

2.1. IMO Requirements

As discussed above the IMO have developed various resolutions that outline the requirements of maritime equipment, including the VDR an S-VDR. Table 2 summaries the key documentation, and lists any requirements related to the security of the devices or the data they store.

These four core documents do little in the way to improve the security of the VDR and the data they store. Whilst the primary resolutions covering VDRs and S-VDRs, MSC.333(90) [2] and MSC.163(78) [26] do mention protecting data from manipulation they do not provide any recommendations on how this should be achieved. What is more, as will be discussed in Section 3, even with devices compliant to these requirements, it was possible to manipulate the data without the attempt being recorded.

The adoption of MSC.214(81) in 2006, appended a new section to the existing requirements, covering download and playback requirements [27]. These requirements state that any device interfaces must be compatible with off-the-shelf operating systems (such as Microsoft Windows or open-sourced Linux/Android), and if a proprietary system or

interface is used, the method of accessing the data should be stored within the VDR. As will be demonstrated in Section 3 the current implementation of this requirement can introduce vulnerabilities to the VDR.

Table 2. Summary of IMO Requirements for VDRs.

Requirement	Name	Security Requirements	Comments
MSC.333(90)	Adoption of Revised Performance Standards for Shipborne Voyage Data Recorders (VDRs)	Resolution states all three recording mediums are "capable of being accessed following an incident but secure against a physical or electronically manipulated changed or deletion of recorded data" Equipment should be designed within the realm of practical possibility, resilient against manipulations of the amount of data, or the data itself. Any manipulation attempt should be recorded.	Provides performance requirements for devices installed after 1 July 2014. For devices installed prior to 1 July 2014 see A.861(20) as amended by MSC.214(81). Amended in 2021 by MSC.494(104) to consider changes in another piece of equipment's performance standards.
MSC.163(78)	Performance Standards for Shipborne Simplified Voyage Data Recorders (S-VDRs)	All recording mediums should be designed in such a way as not to interfere with the integrity of the data, whilst being accessible after an incident.	Like MSC.333(90) covers the performance standards for S-VDRs.
MSC.191(79)	Performance Standards for the Presentation of Navigation-Related Information on Shipborne Navigation Displays	No security requirements	Harmonise requirements for the presentation of navigational-information on the bridge (colours, symbols, resolution etc).
A.694(17)	General Requirements for Shipborne Radio Equipment Forming Part of the Global Maritime Distress and Safety System	No security requirements	Overarching set of minimum design requirements for any maritime device.

Another requirement that whilst not security-focused could have a bearing on the security of the VDR comes under A.694(17). This resolution is one of the oldest in this review, and has not been updated since 1991 [28]. Requirement 3.4. argues that "the design of the equipment should be such that misuse of the controls should not cause damage to the equipment or injury to personnel". Therefore, by extension, the inclusion of USB interfaces on VDRs as a control method, used for updating software, should be done in a way that misuse should not lead to damage. From the ground truth experimentation below, the results will illustrate that the factory-installed USB drive on the VDR could allow an attacker to manipulate the software and data stored directly on the device.

Furthermore, Requirement 8.0 of the resolution require devices to be installed in a manner that they are readily available and accessible for inspection, maintenance, and replacements. Thus, as will be discussed below by devices complying with the high-level requirements of this resolution, it could inherently introduce cyber-risks to those devices.

Of least interest for this review is MSC.191(79) which adds no security requirements to the VDR or its data. The primary reason that VDRs must demonstrate compliance is due to the inclusion of a graphical interface that operations can control and configure the device via on the bridge [29]. However, this could be considered a security requirement, because ensuring a standard, consistent and harmonised user interface for these devices, regardless of the manufacturer should reduce human operating error.

2.2. IEC Standards

One of the core purposes of the IEC standards is to convert the IMO requirements into testable and verifiable requirements. What is more, the standards provide the methods

through which the requirements must be tested to confirm compliance. Table 3 provides details of the key IEC standards that cover the VDRs within this discussion.

Table 3. Summary of IEC Standards Requirements for VDRs [30–35].

Standard	Name	Security Requirements	Comments
IEC 61996-1:2013+A1:2021	Maritime navigation and radiocommunication equipment and systems. Shipborne voyage data recorder (VDR). Performance requirements, methods of testing and required test results	Requirements regarding resistance to tampering, recording integrity and the protection of configuration data are verbatim from MSC.333(90). Additional statement saying data should be protected through the use of "a key, password or similar means" Provides a list of requirements that must be present during an inspection to be considered resistant to tampering.	Standardises the requirements of MSC.333(90), and outlines the required methods to set compliance. For a VDR to be deemed SOLAS Chapter V compiant it must conform to this standard.
IEC 60945:2008	Maritime navigation and radio communication equipment and systems. General requirements. Methods of testing and required test results	No security requirements	Standardises the requirements of IMO Res A.694(17). Specifies the minimum performance requirements, methods of testing, and required results of maritime equipment.
IEC 61162-1 IEC61162-2 IEC 61162-450	Maritime navigation and radiocommunication equipment and systems. Digital interfaces.	IEC 61162-1 and IEC 61162-2 have no security requirements. IEC 61162-450 outlines how a general authentication tag can be added to messages to support the management of cyber security risk (7.2.3.8). No details provided on how this can be used to improve device security of data integrity.	This series covers the digital interfaces between devices. Primarily outlining the standard sentence structures for transmitted data to ensure message cross-compatibility.
IEC 62288:2022	Maritime navigation and radiocommunication equipment and systems. Presentation of navigation-related information on shipborne navigational displays. General requirements, methods of testing and required test results	No security requirements	Standardises the requirements contained within IMO Res MSC.191(79).

The primary document of interest is IEC 61996-1:2013+A1:2021 as this standardises the requirements of MSC.333(90) [30]. While much of the text is directly copied from the IMO resolution there are several notable additions. Firstly, it provides a detailed description of the testing and verification process VDRs must go through to demonstrate compliance. Secondly, the standard identifies a number of other standards that should be consulted, for example IEC 61162 covering signal interfaces. Thirdly, and most importantly for the security of the device, the standard provides a list of requirements that must be present during an inspection to demonstrate tamper resistance. These are:

- access to any physical part of the system, except the data output interface, shall require the use of tools or keys
- any access to the final recording medium shall leave easily recognisable evidence of tampering, e.g., seals or stickers

- operation or any controls or keyboard keys, or any combination of these, shall not affect recording
- termination of recording shall only be possible by means of a key or other secure method
- recorded data shall be protected against unauthorised access by use of a password

Alongside these requirements, the standard also stipulates that to aid the recovery of data from the device a copy of any proprietary software or interfaces within the VDR unit itself. As will be discussed in more detail later, this requirement could have a detrimental effect on the security of the device, whilst not providing clear and significant benefits.

One requirement from IEC 60845:2008, whilst initially a safety requirement could also be considered a security requirement. Requirement 6.2.1.b states that one should "Check that operational controls, the inadvertent exercise of which could switch off the equipment, lead to performance degradation, or to false indications not obvious to the operator, are specifically protected against unintentional operation" [31]. Again, as before one could argue that using the USB interface to update software could be considered an operational control, and as such should have protections against in the inadvertent disruption of the systems.

3. VDR Security Vulnerabilities

As discussed above, the primary regulation covering VDR requirements is IMO Resolution MSC.333(90). The resolution argues that the data should be secured against both physical and electronic manipulation, meaning the VDR should be designed to be tamper proof or tamper resistant, Thus, an attacker should not be able to alter, (1) the amount of data recorded, (2) the data itself, with all manipulation attempts recorded [2]. However, reports indicate that vulnerabilities readily exist in various manufactured VDRs today, and prove VDRs can be tampered with. In 2015, a researcher at IOActive analysed and emulated the firmware and software of the Furuno VR3000 VDR and found vulnerabilities that could be exploited by a remote attacker to access, modify and delete data [19]. Whilst this example is a few years old, and the company has since released a newer version of the device, ship-owners are not mandated to update their devices. Therefore, it is not unfeasible to argue that there are ships in the world fleet still sailing with these insecure devices. A more recent example demonstrates how a vulnerability was found in the Interschalt VDR G4e and S-VDR G4e software, allowing attackers to read and download files from the target system [36]. Published under CVE-2016-9339, the vulnerability has been given a CVSS (Common Vulnerability Scoring System) base score of 5.3 (medium) affecting devices globally [37]. Lastly, a paper on an off-the shelf, non-emulated VDR showed that a VDR by a previously untested manufacturer was also vulnerable to tampering [38].

This study also attempts to find ground-truth by testing an unaltered, off-the-shelf VDR system in order to inform suggested changes to relevant security standards. In these experiments, we found that this VDR, connected to other real systems the way it would be on a bridge, has all the vulnerabilities in the research identified above. What is more, the device in question did not provide any mechanism to verify and check the data for manipulation. Therefore, it raises questions as to how this particular device, or any other existing VDR system, could be considered compliant. Remembering that Resolution MSC.333(90) only provides recommendations, it is the ISO standards that provide the exact performance standards expected. The relevant ISO standards use the term tamper proofto describe the level of security required by VDR data collection and recording processes. Whilst there is no exact definition of tamper proof given in the VDR standards, the following definition is used in a variety of other ISO standards:

> "... designed such that malicious modification or deletion of electronically stored information by subjection to electromagnetic signals from commonly available electronic devices is not possible" [39]

Thus, in practice, manufacturers only have to demonstrate the device is resistant to electromagnetic interference rather than other forms of digital tampering (e.g., use of USB).

As this paper has argued, due to the importance of having accurate incident data, these devices must do more to protect the data stored on them. Therefore, to better understand potential data security requirements it is important to first consider what is meant by information security.

The Confidentiality, Integrity and Availability triad, or CIA triad, is a well-known information security model used to aid the design and development of secure systems and security policies [40]. Therefore, to be considered secure data must be protected from being disclosed to unauthorised users of processes, whilst insuring that any processes that uses this data does not alter it in anyway, or stop it being available. Each of the three elements of the CIA triad is important for a system like the VDR, which holds critical evidence data. A compromised VDR can mean any one element of the triad being affected. As an example, while an attacker can breach the confidentiality by accessing log files or archived voyage data, manipulating or deleting them can affect the integrity of the information. The availability of a VDR is affected by its failure to record or when it has been intentionally damaged to achieve a similar outcome.

While the concept of the CIA triad is that all three are equal, industry priorities may place different importance on each part at a given time. When we suggest solutions we are trying to align these with the perceived priorities of the sector. We assessed this perception from a public forum, the authors asked participants to anonymously vote on the order of importance they would place on these three elements in the context of the VDR. The audience, which consisted of over 100 international maritime and cyber security experts choose the order Integrity, Availability, and then Confidentiality. This demonstrates that in terms of VDR data it is more important to have data that can be trusted over data that is kept secret. While this perception may not be critical in technical solutions to VDR security, this may be more critical in understanding sector wide concerns and demands when considering changes in standards.

3.1. Determining the Information Security Properties of a VDR

To understand the VDR cyber-vulnerabilities and how these could affect the CIA triad, the authors performed a penetration test (pentest) on an off-the-shelf VDR produced by a global manufacturer. The purpose of testing is to realistically determine the actual risks of VDRs, and effectively promote high-impact changes to the relevant standards.

The VDR under test, hereafter VDR_T, ran on Windows Embedded Standard 7, a Microsoft OS released in 2010. More specific details regarding the model is omitted for security purposes. It is indicative of the maritime sector that these devices remain compliant, and in use, even though support for the OS (including security updates) was terminated in 2020 [41]. An external attack machine running on Kali Linux OS (Kali being a variant of the popular Linux OS) was used to perform attacks and tests. The Kali Linux operating system distribution is designed specifically for penetration testing with pre-configured tools and functionalities to run custom scripts [42].

To demonstrate the ease at which an attacker could target VDR data a range of publicly available tools were used during the penetration test. The first tool was Nmap or Network mapper, a publicly available network scanning tool used to discover the hosts on a network [43]. Nmap gathers information about a network such as host names, port numbers, services running on them, and operating systems. Using this information informs the development of further tests.

The next tool that was used was the Metasploit framework, containing modules for identifying weaknesses in a system and the exploits that can be used to target them [44]. Thus, with the information gathered from the Nmap scan, exploits can be found that specifically target the OS of the device. This scan also highlighted the make and model of the device, which then pointed to the open USB interface built into the device, so to ensure the delivery of the malicious payload a $59.99 USB Rubber Ducky was used as the attack vector. Once inserted the Rubber Ducky injects keystrokes [45] which digitally imitates a user physically typing in commands via a keyboard [46,47]. Scripts of these keystrokes are

pre-loaded onto the USB by the attacker allowing the USB to execute commands on the device automatically when plugged in. These devices do not require complicated technical knowledge to be used, and can be extremely dangerous when properly configured.

Two of the payloads that the Rubber Ducky executed were the Shinolocker Ransomware Simulator and a Reverse TCP shell. Using Shinolocker, an attacker can create a custom payload to encrypt files, limiting the users' ability to access them. Recent years have seen an increase in ransomware attacks, and according to a study by Sophos, the average ransom paid is around $812,360 [48]. Since 2017, all four of the major shipping companies (CMA CGM, APM-Maersk, MSC and COSTCO) have been impacted by a ransomware attack that has disrupted their operations for days [49]. Therefore, it is important to understand the consequences of such an attack on the VDR. A Reverse TCP shell payload will initiate a connection from a target machine to an attacker's machine, granting the attacker access to the target machine's files and folders. With access to these files another tool, Hydra, a password cracker, can be used to perform brute-force attacks on stored login data to retrieve the right username and password combinations [50]. With access to these password combinations an attacker could gain legitimate access to the system, its configuration and the data it is storing and move through the system as though they were meant to be there being given full rights and access of the user they are impersonating.

3.2. VDR Vulnerabilities

This section contextualises the pentest results on the VDR_T against each of the CIA triad elements, and how the system responds to them. It is important to note that the authors opted to use off-the-shelf tools and functionalities to best demonstrate the vulnerabilities found within these devices. Arguably, if custom tools had been required to exploit vulnerabilities, then this would demonstrate some inherent security mechanisms in the device. However, the use of standard tools illustrates the ease at which an adversary can target these devices successfully, often requiring limited specialist skills, costs, time, or equipment.

3.2.1. Confidentiality

An initial step in penetration testing is reconnaissance of the target system. To understand the target device, in this case VDR_T, the network was scanned using Nmap. This scan identified the operating system (Windows embedded standard 7) and additional services running on the VDR, providing details like the MAC address, the type of device, and the open system ports. The scan also found that the SMB port (Server Message Block) was open.

Using a scanning module within Metasploit called '`smb_enumusers`', five unique user accounts were identified within the VDR, demonstrating a compromise in the confidentiality of the data within the VDR. With this list of users, Hydra could be used, in conjunction with a common password list, to perform a brute-force attack to obtain passwords for the user accounts 'Administrator' and 'Captain'. The remaining three accounts had blank passwords, including the 'administrator' account. These accounts were not created by the authors, but existed on the VDR when it was acquired. As a result, this provided the authors, who again did not create these accounts, access to these five users' files and user account privileges, which, because of their roles and responsibilities on board, meant they had some of the highest privileges available. These privileges granted access to account configurations, systems settings and logs, in addition to access to the voyage data.

A second vulnerability identified in the Windows OS on VDR_T was the EternalRomance exploit, which was used within the NotPetya attack that hit Mærsk in 2017 [51]. When executed successfully, EternalRomance exploits a vulnerability in SMB protocol to give the attacker control over the target computer [52]. Used in conjunction with the previously retrieved usernames and passwords, the authors were able to view and access all files and logs on VDR_T. This data includes the voyage data archives which include Radar screenshots, audio recordings, and NMEA data. NMEA data is the National Maritime Elec-

tronics Association standard for electrical signal requirements and data transmission [53]. As data is recorded in a standardised format, it allows an attacker to know the exact contents of the message strings, and make changes to these. Thus, users with read and write privileges to these files compromise both the confidentiality and integrity of the data. Manipulating the NMEA data by changing values like geographic location can affect an accident investigation negatively as these messages are used to construct and trace the voyage details during further inquiry.

3.2.2. Integrity

Manipulating the data stored in the VDR_T affects the data integrity element of the CIA triad. To test the effects of compromised integrity, a Reverse TCP shell was created. Reverse shells are connections from the target system (VDR_T) to the attacker's system (Kali) that allows the attacker to access and control the target system. Once the payload was executed on VDR_T, the attacker received remote access to the system with local user privileges, which allowed the attacker to view and access the files (see Figure 2). An escalation of privileges was then performed, and five password hashes were extracted. These passwords were the same ones as the ones extracted earlier, just via a different attack route. As with the exploitation of SMB vulnerabilities mentioned in the previous section, gaining these password combinations allows an attacker to enter the system and access a number of folders, sub-folders, and files, including the voyage data.

Voyage data is archived every minute as zip files, as shown in Figure 3, with NMEA messages in a text file (1), a one-minute audio clip from the bridge (2), and four RADAR screenshots captured at an interval of 15 s (3). Each archived zip file is uniquely named and easily identifiable. NMEA messages are stored in plain text format, meaning they are easier to alter. The messages include a checksum as a way to ensure no errors in the data occur during transmission, which can provide a rudimentary form of integrity checking. However, this can be altered as well, so is of limited use when trying to verify the integrity of the data. In essence, a rudimentary checksum can be forged, the way a physical seal or sticker could be. However, a hash, like most modern seals and stickers, are designed to be less easily forged.

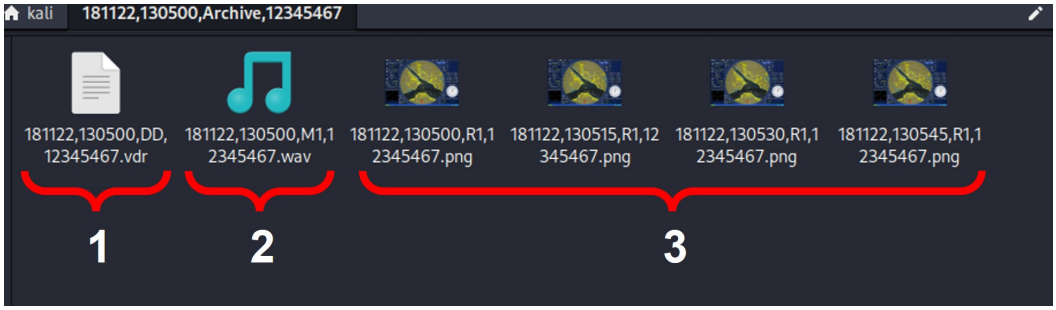

Figure 3. Example archived zip file with three types of voyage data.

The only indication of information alteration on the VDR_T was the MACE (modified, accessed, created, entry modified) time values. The MACE values are the timestamps of the latest modification, last access, creation of file/folder and entry modified [54], which are details required by VDR standards. To hide the trace of modification, MACE values can be changed to any other value as the attacker wishes, which may compromise an accident investigation when the VDR is involved. After manipulating NMEA messages and voyage data, the MACE values of the file was changed to a different date and time using the reverse shell's Timestomp utility. This means that the attacker can get away with manipulating evidence data without leaving a trace, which directly contravenes the IEC 61996 requirement to leave clear evidence of tampering.

3.2.3. Availability

The availability of VDR data and the system itself is vital for maritime casualty investigations and as highlighted throughout the standards the ease at which this data can be obtained is critical. There are several factors that can affect data retrieval and availability, including trouble finding the VDR, damage to the recording device, paused recording, and deletion of data (intentional or unintentional). The scope of this paper is limited to intentional electronic actions that affect the availability of data. However, there are examples where users have failed to manually save the data during an incident [55], which can be looked up unfavourably in investigations suggesting the user is trying to hide something [56].

Ransomware attacks are among the most common attacks against maritime industries, as discussed in Section 3.1. To test how a VDR would react in the event of a ransomware attack, the authors used the Shinolocker ransomware simulator. In all experiments, this tool demonstrated that the ransomware was successful in removing the availability of files within VDR_T, until the ransom was "paid", and the decryption key was provided. The simulator provides these keys, demonstrating availability can be restored.

However, in these situations, it is of interest to see if the authorities pay the ransom to retrieve the evidence data back in the event of an attack, and even if they do, if all the data is returned. In a report by Sophos on ransomware, 46% of the respondents paid ransoms to get their data back; however, only 4% of those who paid, got all their data back [48], which directly impacts the availability of the data. What is more, this could also lead to a compromise in the chain of custody of the data in an investigation, as questions could be raised regarding the integrity of the data after a malicious 3rd party demonstrated the ability to access and potentially alter it.

EternalBlue, similar to EternalRomance but famous for its use in the 2017 WannaCry ransomware attack [57], was another exploit used to leverage the vulnerabilities in Windows SMB protocol. Using this exploit caused the VDR_T to crash. This specific type of crash indicates a fatal error in the systems operations and has to shut down, a state that often requires further analysis to determine the cause. In this case, it was necessary to manually reboot the VDR_T in order to restore its functionality. Performing such an attack on the VDR can stop it from recording and it will stay that way unless someone notices it and reboots it. This is a form of denial of service, and tampering with the recording part of the device, whereas the ransomware tampered with the storage component of a VDR. This affects the availability of a service, as opposed to the availability of the data.

Previous work, mentioned above, has also shown it is possible to completely erase the hard drive. However, this attack was not performed on VDR_T, as it would cause problems for future use and testing. That said, it has been shown to be possible, and destroying all the evidence data on a hard drive represents a clear and serious case of denial of service, affecting the availability of information and can prove catastrophic in high-profile investigations.

3.3. Summary

The attacks presented demonstrate how easily accessible tools can compromise the confidentiality, integrity and availability of VDR data and services. As discussed, the use of publicly available tools increases the risk to the security of the VDR, as an attacker does not need to craft or develop special tools to manipulate the vital information stored on the device. This section has demonstrated that both the deletion of data (hard drive erasure) and the manipulation of data by hiding the trace (manipulating NMEA data) is possible. Remembering that MSC.333(90) stipulates that these devices, and the data they store, should be secure against physical or digital manipulation. Thus, our test demonstrates that compliant VDRs do not fully achieve this requirement.

Whilst not considered a critical navigation system in IMO regulation, when asked at the same public forum above experts identified the VDR as critically important to incident investigation, providing an average criticality rating of eight out of ten with no responses less than five. The manipulation or loss of data could have a negative impact on those

investigations. Depending on the situation, this could have a direct impact upon legal proceedings as the data (i.e., evidence) is not available, or if its integrity is under question. Arguably, this could have a low impact on investigations as authorities would seek information from other sources e.g., witness statements or system logs. However, the carriage of the VDR was mandated to ensure these other potentially unreliable sources were not relied upon. Moreover, if VDRs are used on autonomous vessels, digital information could be the only form of evidence available.

The attacks demonstrated in this paper also highlight how requirements, like those found in MSC.163(78), expose the VDR to other vulnerabilities. Consider the requirement to use common interfaces and operating systems; If proprietary interfaces or software is used, the method to access the data must be stored within the VDR itself, as mandated under IEC 61996-1. Therefore, as most VDRs and devices used to update or download data the VDR use standard USB interfaces, there is little to no security benefit to using a proprietary interface. A determined attacker could just use the USB to proprietary interface converter lead mandated to be stored physically with the device. Remembering also that Resolution A.694(17) stipulates that the misuse of control should not damage the equipment.

It could be argued that, in the case of the VDR, the USB interface is a control mechanism (i.e., used to update software). Therefore, the USB attacks demonstrated above illustrate that again the VDR does not fully adhere to this requirement, and fails to meet the expected performance requirements of IEC 60945. The following section will discuss how these requirements could be adapted to increase security whilst ensuring the required access.

It is also worth noting that the security requirements laid out in IEC 61996-1 (Section 2.2) do little to improve the overall security of the VDR. For example, the requirement for the use of key or tool for access only covers the physical components, not the data output interface. The use of stickers/seals to show tampering add not discernible security against this type of attack which uses the accessible interface. Finally, the termination of the recording must only be possible via a key or secure measure. This requirement is too broad because the deletion of all data, while technically not terminating the recording, would have the same effect on the data being recorded.

In conclusion, this paper has highlighted that, while the international requirements and standards published by the IMO and IEC do provide a minimum level of quality to VDRs, they fail to insist on security being included. The high-level approach is understandable as these requirements are developed through the means of consensus ensuring they can be implemented without discrimination. However, the requirements do not consider (1) the complexity of digital technology found on board and (2) the capabilities of adversaries.

4. Raising the Standard

The position of this paper argues that the current performance standards covering maritime VDRs do not instil a sufficiently high level of security in these devices, leaving their data and services open to tampering, i.e., manipulation or deletion. There are several factors that play a key role in this lack of security focus. Firstly, dating back to its inception, the IMO is primarily a safety-focused organisation set out to ensure the safety of the seafarers, ships and the environment [58]. Therefore, as illustrated by many of the requirements listed above, the focus of its governance of VDRs is on how these devices can be used to improve safety i.e., they have detailed information about incidents to ensure they do not happen again. Secondly, the IMO has only recently explicitly included cyber risk management within its governance. MSC.428(98), entered into force on the 1 January 2021, so companies are only at the beginning of their journey to understand cyber risk within their operations [59]. Thirdly, as highlighted by the earlier standards review, organisations like the IEC look to governing bodies like the IMO to provide the high-level requirement goals. The standards are therefore the means to achieve the requirements listed by the governing body. Thus, the standards rarely introduce a higher level of requirement than is already agreed upon by the international community within the regulator, and in this case, they remain relatively vague in terms of security.

It was indicated at the start of this paper that the definition of 'tamper proof' in the VDR standards is vague and does not address information security aspects, or the new threats posed by the integration of digital technology. With more and more devices becoming digital and connected, it is becoming increasingly necessary to define these terms to be considerate of electronic and remote tampering as well as cover information security. This is not arguing for a complete change in definition for tamper proof but rather a re-imagining using, for example, the phrase already used in MSC.333(90). Therefore, the essence of tamper proofing to ensure information security should be that "... equipment should be so designed that, as far as is practical, it is not possible to manipulate the amount of data being recorded by the VDR, the data itself nor the data which has already been recorded." [2]. Changing the definition to the suggested would make information a central part of VDR performance requirements, and ensure that manufacturers are obligated to consider the forms of manipulation and deletion discussed in this paper.

To achieve this style of tamper proofing more work would need to be done in the sector to consider tamper proof devices. Whilst the authors appreciate that these devices are not critical to navigation, or the safety of the vessel, it is important to consider how these devices are integrated within the ship's network, and the risk this poses to other, more critical, systems. "People", "Process" and "Technology" (PPT) was originally a thought process designed by car manufacturer Toyota to understand the product development process [60]. However, now PPT is now used by companies to understand how the three elements interact with each other. As such [61] argues that successful information security hinges upon the proper integration of PPT. Therefore to improve the security of VDR data, to ensure it cannot be manipulated or changed, a variety of methods can be implemented, including the physical security of the device (e.g., location), access control to devices and interfaces (e.g., separate control ports), secure physical modules (e.g., chip board coating and sealing) and cryptographic principles (e.g., hashing and encryption) [62,63]. To this end, this section will lay out a variety of different measures that manufacturers, or users, could implement that would help to improve the security of the VDR. These suggestions are not intended to reinvent the wheel for information security. Rather, the suggestions will be based on other standards, particularly those focused on information security. Thus, would not require the complete re-writing of the VDR standards just an appropriate cross-reference, which is standard practice within these standards. If integrated as performance requirements within the VDR standard, these suggestions would go a long way to improve the security of the world's fleet.

4.1. Components of VDR Security

4.1.1. Physical Security

The attacks demonstrated above illustrate how through direct access to the VDR an attacker is able to access and manipulate the operating system and stored data. More could be done to physically secure these devices. However, currently the standards inhibit many improvements in security via physical means. For instance, Annex C of IEC 61996-1 stipulates the data port "shall be easily accessible" [30]. Therefore, there are limitations on how to physically secure this port without it becoming "easily accessible". One solution would be to make access to the actual device harder i.e., locating it within a locked cupboard. However, this could breach the ease of access requirement. One potential solution can be found within IMO A.694(17). In this case, the resolution discusses the need for using tools like a spanner or screwdriver to access parts of equipment that use high voltages [28]. Therefore, the same could be used alongside a key as a way to protect the data port and physical hard drives of the VDR. The key would be easily available, stored on the bridge near to the VDR, but separately, increasing the number of steps required to gain access to the device.

Another solution to increase security, as suggested by [64] would be physical location of the device. Whilst IEC 61991-1 outlines requirements for the installation locations of various parts of the VDR these primarily cover the fixed and float-free recording mediums.

The location of the core module, and data interfaces could be within high-traffic areas, which are already covered by other access control mechanisms. For instance, within the bridge, which under the requirements of the International Ship and Port Facility Security (ISPS) Code must have procedures in place to limit unauthorised access [65], decreasing the opportunity for an individual to access the device, and to be alone with the device. Ref. [66] provides clear and concise requirements regarding access control not just to data but also to physical assets. Therefore, to facilitate an improvement in the physical security of VDRs the current requirements need to be amended, or removed allowing for improved requirements, like those found in ISO27001, to be implemented.

4.1.2. Data Security

As illustrated the use of generic interfaces like USBs for software updates and data downloads opens VDRs to a range of vulnerabilities. Potential mitigation to this is the use of proprietary interfaces or software. The use of such a measure would mean only those with direct physical access to the device, with the correct connection device/lead would be able to access the data stored on the device. Whilst not removing the threat completely it would still help to mitigate some of the risks found with using a USB interface. However, as with physical security, the current requirements of MSC.333(90) and MSC.163(78) set specific requirements in regards to the ability to download and playback VDR recordings that directly inhibit improvements in security [2,26]. The requirements of the Resolution's clearly state that the interface should be comparable with an internationally recognised format, such as Ethernet, USB, FireWire or equivalent. The same is true of the software program required to playback recordings, this must be compatible with commercial-off-the-self operating software. Furthermore, if a proprietary interface or program is required this must be provided on a portable storage device at installation and stored within the main unit of the VDR. Therefore, the requirements prohibit the use of proprietary equipment as a security measure.

However, requirement 5.5.3.a of IEC 61991-1 stipulates that instructions to enable the manufacture of special tools or interface equipment for retrieval of data, and details of necessary actions to be followed for data retrieval should be available to investigation authorities [30]. Therefore, arguably as long as instructions are left on the type of interface required, or where the software needs to be downloaded from, an extra level of identity verification can occur. By requiring investigators to contact the manufacturer for a copy of the interface or software, it would allow their authority to be confirmed prior to providing the information. This verification process could include the need to provide details about the device in question (i.e a unique identifier stamped physically onto the unit), as well as proof of their authority (e.g., registered with the national governing body). Furthermore, any software required to access the data could require the use of passwords which, as will be discussed below, could be part of a Multi Factor Authentication (MFA) scheme or of a tamper evident design. Even if the proprietary software or interface is stored within the VDR this could be done in a way to further improve security. For instance, the physical location of the tools required to access the interface converter.

4.1.3. Cryptographic Methods for Integrity Checking

In the past, cryptographic methods such as hashing and encryption have been suggested to verify the integrity of information while it is in transit or at rest. Whilst the physical security, and access control mechanisms suggested above are relatively simple to implement, the use of cryptographic techniques is more complex and requires more work to ensure its effectiveness. Whilst cryptography has primarily focused on securing data within IT systems [64] has illustrated how it can be applied to industrial control systems.

There have been some attempts within academia to explore this previously, for example [67] proposes a hash-based method to verify the integrity of VDR data. Using the NMEA messages from the transmitter, this method creates a secret key that is combined with the message, into an authentication code using a specific algorithm. The authenti-

cation code is then saved, so that when data from the VDR is processed in the same way, the authentication codes can be compared to ensure they match. This method has been tested using Global Positioning System (GPS) data where the secret key is created using the time and date information from NMEA GPS messages [67]. The use of a secure hashing mechanism can confirm that the data has not been manipulated.

Additionally, some image hashing techniques can be used to help secure Radar screenshots on the VDR against manipulation. In one study, hashing and watermarking were used to protect a few image files from tampering [68]. First, a standard hashing algorithm (Fast Johnson Lindestrauss Transform—FJLT) is used to create a hash value, which is then embedded onto the image as a watermark using another standard robust technique (Discrete Cosine Transform—DCT) [69]. The watermarks are then embedded using a blind watermarking process which means the data is hidden within the image making it invisible to the user/attacker and the original image is not required to extract the watermark for comparison. To verify the integrity of the watermarked image, the receiver generates a hash using the same algorithm and compares it with the hash extracted from the watermark [68]. Additionally, there are some studies that support the use of watermarking for multimedia data, including [70] which proposes a method for watermarking satellite images, and [71] which conducted a literature survey on watermarking for medical images.

As argued by [62], any device that contains components of cryptographic methods must be both physically and digitally secure. If an attacker were to gain access to these components it would enable them to undermine any of the hashing or encryption methods, allowing them to manipulate the data as before. Within the automotive sector [63] proposes having a Tamper Proof Device (TPD), a hardware security module device, that stores the authentication keys to identify each vehicle and their drivers, which when compared to the VDR, can be the keys for authenticating the bridge devices and verifying their data. An example of a similar solution is proposed in Figure 4 to increase the security of VDR data using cryptographic methods. Figure 4A provides an option to verify the integrity of data using a separate hashing device that is connected parallel to the VDR. As the data is processed by the VDR, it is also passed through the hashing device. Data hashes will be created by this device and stored on storage mediums alongside the original data. During an investigation, the authority will be able to retrieve the original data, hash it, and then compare it to the stored hash. Although this does not guarantee that the data will not be tampered with, it will provide a way to confirm if it has.

Figure 4B shows a retrofitted encryption device for the VDR. Data from the sensors and bridge equipment are first encrypted using a standard algorithm (for example AES 256 [72]) by the encryption device, then processed by the VDR and stored as normal on the storage mediums. A key advantage of this is that it ensures data confidentiality and makes it harder for attackers to read and tamper with it. The primary concern with these security methods is that they could breach the ease of accessibility requirement, whereby decryption keys are only made available only to investigators or manufacturers when requested, not stored on the device. However, by following requirements set out in ISO 27001 for key management [66] these methods should not overly inhibit accessibility when required.

Another way to manage the decryption keys, whilst increasing security without hindering accessibility excessively would be through the use of split keys. A split key enables the splitting of one decryption key into multiple keys and storing them in different places. In this way, even if a part of the key is intercepted, an adversary cannot access the data. For VDRs, split keys can be used to encrypt data, with part of the key held by the manufacturer and part held by the shipping company. As part of an accident investigation, the UK Home Office's Code of Practice for Investigation of Protected Electronic Information requires that the holders of keys be notified to act together and provide the necessary requirements or to disclose the key to the investigators [73]. Therefore, there is already a precedent for this form of security method, and key management to occur. It is important to note that these methods do not stop the deletion of data (availability) they are designed, but if implemented correctly, can ensure the integrity and confidentiality of data.

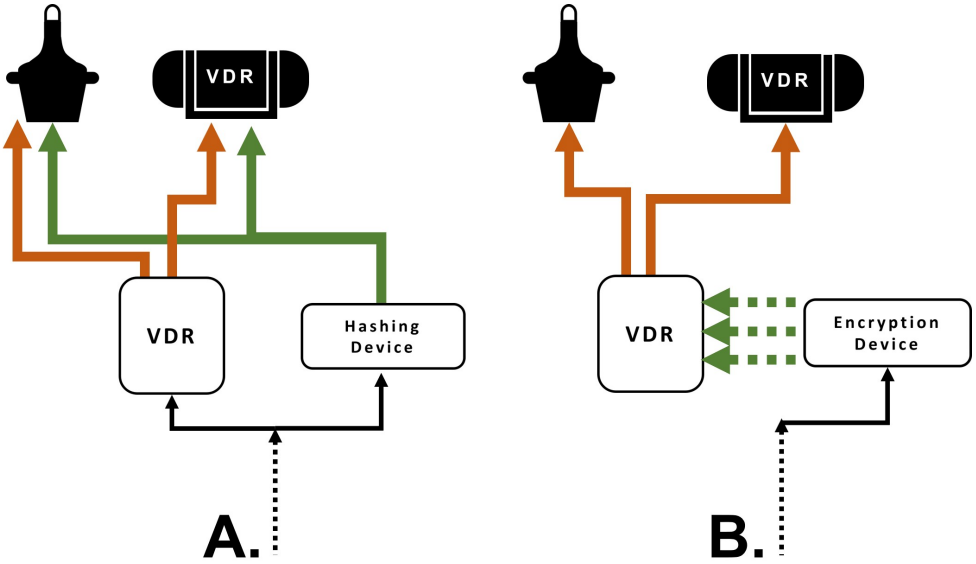

Figure 4. Cryptographic methods for VDR security. (**A**) Storage of a hash of sensor input for verification, (**B**) Encryption of sensor data prior to VDR processing

4.1.4. Password Security Policy

Several of the attacks demonstrated in this paper could have easily been mitigated through the implementation of passwords. As discussed IEC 61996-1 stipulates that recorded data should be protected against unauthorised access by the use of a password. However, this requirement focuses on the data, and not the operating system of the VDR. Without strong passwords, the experiments above illustrate that the attacker is able to directly manipulate the unprotected data stored by the operating system in ZIP format. What is more, where passwords were being used they were either incorrectly set up (e.g., blank passwords) or using simple, and easy-to-break phrases. For example, in VDR_T the user account 'Engineer' used the password 'Pugwash1', which is a popular British comic strip character and animation featuring a pirate called Captain Pugwash.

The use of passwords is not a new concept in cyber security and is still the most widespread authentication scheme [74]. The use of a simple alphanumeric password would reduce the ease at which an attacker could manipulate files [75]. However, passwords are not a silver bullet in terms of security, and as [76] highlights there are many methods that can be broken or guessed. Thus, in the Guidelines on Cyber Security Onboard Ships they urge operators to consider MFA [77], whilst NIST recommends the use of active password checkers that inhibit weak, or recently used passwords [64], making access more complex [77]. One example of MFA would be the requirement of two passwords to enable access. For instance, the use of a memorised passphrase and a code from 3rd party authenticator app, for example, the Microsoft Authenticator app [78].

If passwords are to be used it is important to consider the implementation of a policy within the company that covers the creation, and use, of passwords. A password policy explains what the rules and expectations are in regard to passwords, what is more, it provides a framework through which enforcement can occur [79]. Looking at the standards, password policies should adopt requirements for passphrases that include, for example not being dictionary words, and not containing repetitive or sequential characters [80,81].

However, as highlighted above, any proprietary software or interfaces needed to access the device, which could include passwords, needs to be physically attached to the VDR or hard-coded into the device. Therefore, requiring a password for access to this software and data would inhibit investigations and could be non-compliant with the standard. Considering [82]'s argument that, in some circumstances, it might be preferable to use a less secure security scheme that is designed to be usable whilst creating a false perception

of security to outsiders. With this concept in mind, there are possible workarounds which would allow the use of passwords to become required without affecting access.

For instance, consider the use of a tamper proof password device physically secured within the VDR. Popular media famously depicts these "snap-to-open" cases as containing the launch codes for nuclear arsenals. Whilst there is evidence that these devices are used in protecting nuclear launch codes [83], there are limited commercially available options (see [84]). However, this is not to say a cheaper alternative is not available to manufacturers e.g., the use of a tamperproof envelope and tape etc. For those wishing to take a leaf out of the nuclear protection playbook, [85] illustrates a simple design that can be created on an economical 3D printer. This method does not make access to data harder as the code required to access the device is readily available with the device. However, by it being contained within a case which shows clear evidence of tampering, increases the perception of security. This type of tamper evident design, i.e., the use of seals or stickers to show evidence of tampering, is already approved under IEC 61996-1. As such, would only require small changes in technical and physical design to implement.

4.1.5. Update/Patch Policy

Based on the vulnerabilities and attack vectors we examined, it is evident that update and patch management plays a critical role in system security. To protect against outdated systems with many published vulnerabilities and zero-day exploits, patches and system updates are necessary. For VDRs, it is important to consider standardised patching policies that determine who, what, when, and how it is applied. It is necessary to prioritize the assets that need to be patched and then schedule the patching correctly. In most VDRs, software updates are performed through USB, but because of the threats introduced through the USB ports, there needs to be some kind of control. In addition, VDR standards do not specify a time frame for updating the OS, which can have huge consequences in cases where there is a critical security vulnerability found within the operating system. During the period of the system update, it is also necessary to consider how the recording and operations will take place.

As [86] argues, patches could be the cure to many software vulnerabilities if it was not for various issues. Firstly, patch management is multifaceted and there are often too many vulnerabilities to patch at once. Take for example Microsoft's Patch Tuesday where multiple patches are applied on a single day within one release. Rather than being shipped-when-ready, which led to issues where people were never sure if they were turning their devices on to find it needing multiple patch installs [87]. Secondly, patches need to be tested within their operational environment first to ensure that it does not conflict with existing operations. Thirdly patches often require installation which means shutting the system down and restarting it. In the case of the VDR this could require the device to stop recording for that period of time, which would impact the times at which the device could be updated.

Further to this the IEC 62443-3-2:2020, covering security for industrial control systems, argues that details about the system (i.e., software version etc.) and its integration should be documented and accessible when required [88]. ISO27001 argues that information about systems vulnerabilities should be obtained in a timely fashion and vulnerabilities accessed and recorded [66]. These documents should then be updated as and when required to ensure they remain consistent with the actual system integration/configuration.

Whilst not having a direct impact on the CIA of VDR data, patch management and policies have an important role to play in information security. The use of management policies like these will ensure that all individuals, both ashore and onboard are aware of their roles and responsibilities for these systems. Under Resolution MSC.428(98), cyber risk management responsible personnel should be identified ensuring they know the important link between updating systems and security. What is more, ensuring responsibilities are clearly defined ensures that these new work processes are built into their current operational practices.

4.1.6. Incident Response and Management Plan

While it is not possible to anticipate and prevent every cyber attack on a device or environment, it is possible to better prepare for them and reduce their consequences. As with any other industry, the maritime sector too requires a proper response plan to cyber incidents. This involves identifying threats, responding to them, communicating with others, and cleaning up afterwards. The NIST SP 800-61 computer security incident handling guide document divides incident handling into four phases: preparation, detection, containment, eradication, and recovery [89]. BIMCO's document on cyber security onboard ships suggests transferring the NIST cyber security framework phases to ship cyber security [77]. When it comes to VDRs, there are two scenarios to consider. One is how incident response activities on board the ship affect the VDR and if the incident details are securely logged when a cyber event occurs on a piece of equipment on board the ship. Secondly, when a cyber attack occurs on the VDR itself, how to effectively protect the data it holds, how to back up and prevent the spread of infection.

Whilst none of the attacks illustrated within this paper demonstrate propagation beyond the VDR and its data, it is important to remember that VDR_T was running on a Windows-embedded standard operating system. The OS, coupled with various multi-directional data interfaces (e.g., Ethernet) could offer an opportunity for an attacker to use the VDR to spread through a ship's network. Thus, operators must be aware of what cyber incidents they could face, and the impact they could have on not just the critical navigation equipment but also on secondary systems like the VDR. ISO 27035 offers guidance on information security incident management and reiterates the importance of defining the roles and responsibilities of those involved in operating and managing digital assets [90].

4.1.7. Security Training

Seafarers need cyber awareness training to understand their environment and the cyber threats they face. Standards and regulatory requirements provide the minimum requirements to be followed, but security training guides them to act better and operate systems more effectively. BIMCO's Guidelines on cyber security onboard ships document identifies the need for training personnel operating IT and OT systems and the training level, as a basis for cyber risk assessment among several others [77].

The United States Coast Guard (USCG) argue that the capitalization of cyber skills is crucial for the continued safety and security of the maritime sector [91]. Further to this, the USCG released Work Instruction (WI) CVC-WI-027(2), covering vessel cyber risk management. The WI indicates the basic level of cyber skills crew members are expected to demonstrate to ensure they are aware of the cyber risks they and their vessel face, and how best to respond to incidents [92]. These requirements are based upon the NIST Cyber Security Framework, whereby security awareness and training are a fundamental component of 'Protect'[93].

The Enrica Lexi case was an infamous shooting incident when two fishermen onboard the fishing boat 'St.Antony' were killed off the western coast of India [94]. Court proceedings describe the duty officer as stating that "he did not press the VDR for recording since it was not a suspicious boat and just a normal boat" [55]. Although the VDR was recovered, the report says that the captain "failed to preserve" the evidence [55]. Considering that the VDR data is automatically saved, it is debatable why it needs to be pressed for recording. In our review, we found that many VDRs on the market have a separate 'save' button that stops the recording on the hard drive, which is an extra precaution to ensure data is saved [95]. As soon as the save button is pressed during an incident, the recording is stopped to prevent overwriting and the incident data is preserved [96]. Despite the fact that the mechanism ensures the availability of evidence, if the crew members are not trained properly to deal with incidents and operate the systems, the technical security measures will fail.

What is more, this again provides clear evidence that the social norm within VDR operational practices is determined by the technology of the past. Understandably when

storage devices had limited capacity ensuring data was not overridden was a key concern. Now storage mediums no longer have these limitations, VDR_T had a 1 TB hard drive large enough for a year's worth of recordings, so there should be no reason for those on board to manually save data. Rather than having the ability to terminate recordings, the manual save could still be implemented, but it could be used to initiate a form of marker within the data so that investigators have a clear indication of where the data important to them starts.

Many of the suggestions listed above require some form of training to ensure they are implemented successfully. Security training more broadly, as well as cyber security specific training is required to ensure the crew are aware of the risks they face, and how their actions, both positive and negative, can impact security. As mentioned, the operators should be aware of their roles and responsibilities, and provided with the skills to ensure they are capable of fulfilling them [97]. For example, understanding the role of passwords, how they form a part of the wider access control policy and what the consequences of sharing login credentials can be.

4.2. Discussion

A change in the performance requirements of these devices arguably is not an easy process, nor a fast one. Moreover, a change in the requirements would also require a change in the annual performance checks of these devices. Under the current guidelines listed by the IMO in MSC.1/Circ.1222/Rev.1 [98], there is no requirement to check the integrity of the VDRs software, or data collected. The testing requirements require confirmation that the device records the appropriate data for the required time period, but there is no comment on its accuracy, or whether this is verified. Therefore, as this section will argue new requirements should be included within these tests to ensure that the digital security of these devices is also checked periodically.

It is important to note that whilst cyber security may be in its infancy within the maritime sector, compared to others like aviation, it is gaining momentum with more organisations considering the impact of cyber risk on safety. Both the IEC and The International Association of Classification Societies (IACS) are such organisations considering the specific risks cyber brings to the maritime sector. In 2021, the IEC released IEC63154:2021 entitled Maritime Navigation and radiocommunication equipment and systems—Cybersecurity. This technical standard is aimed at improving the cybersecurity of any shipborne navigational equipment listed in SOLAS, which the VDR is. None of the devices considered for this paper were compliant with this particular standard due to the devices being certified prior to the release of this standard. The standard consists of 16 Modules, each dealing with a different aspect needed "to provide a basic level of protection against cyber incidents" [99].

Whilst all modules would need to be addressed to achieve compliance, there are several of interest that attention should be drawn to. Firstly, Module C User Authentication argues that users should be required to authenticate themselves via the use of usernames or access cards alongside a password. These passwords, like the requirements mentioned in Section 4.1.4 should be of a minimum length with certain restrictions being enforced. Module J Interfaces for Removable Devices Including USB provides details of how to protect USB ports which are accessible, like those found on the VDR. This security can be achieved through both physical and operational protection measures. The primary mitigation measure of choice is to reduce the ease of access to the ports through the need of a key or tool. However, as discussed above there could be some contention with trying to comply to this requirement and the ones within the specific VDR standards that argue the interfaces must remain easily accessible.

There are some requirements, like those found in Module D 'System Defence'which would be harder to implement in the case of the VDR. As the VDR has an accessible interface that malware could penetrate, the device must be hardened to cyber attacks through the use of either anti-malware software or a firewall. Protection via a firewall would have a limited impact on security as many VDRs use NMEA transferred over other

communication channels (not IP), which a firewall has limited capability of scanning, filtering and dropping communication messages. This would require careful calibration and integration to allow the firewall to effectively serve this security function. This leaves anti-malware software, as the alternative. Whilst the underlying Windows OS is capable of running anti-malware software, which would catch some of the known attacks on these devices, it could also introduce new risks. For example, to ensure the anti-malware remains up-to-date, and therefore an effective line of defence, it requires the crew to update the software regularly. Realistically this could be achieved in two ways, (1) by crew plugging in a USB and updating manually, or (2) updates being applied remotely which would require the device to be connected to the internet. Thus, to ensure this mitigation remains effective, the device would need a greater level of physical or digital connectivity than it currently has.

As with all standards, this remains voluntary, and it is the device manufacturers' choice whether they wish their devices to comply with this standard. In some cases, it might be too great of a challenge both technically and financially to justify the need to comply with these requirements. Secondly, this standard covers the device itself and not the environment it is being integrated into. For example, throughout the standard there is a reference to the manufacturer providing installation instructions to the system integrator. However, if the integrator does not install it as per those instructions, the device itself will be compliant but the system/network/environment it is installed within is not. Thus, means that the device compliance, and its additional security, is not necessarily contributing to the whole system security. Take the secure case for keys to access the interface, if these are provided with instructions the device can be compliant with the standard, but if the integrator does not install or locate the key case appropriately, then the security benefits are negated. Therefore, the introduction of this standard might have a limited benefit on the security of the VDR.

The second organisation giving serious consideration to the cyber security of maritime devices is IACS. IACS, is a technical non-governmental organisation which aims to "... establish the minimum technical standards and requirements that address maritime safety and environmental protection..." [100]. Importantly, the Classification Societies that form the membership of IACS are the organisations that issue ship Class and Compliance certificates, without which ships would not be able to sail. In simplistic terms, the Classification Societies can be seen as an enforcement agency for the IMO, whereby it is against their requirements ships are classed as seaworthy.

In April 2022 IACS released two new Unified Requirements (URs) that focus on cyber security on ships. URs are adopted sets of requirements that all members of IACS must implement as a minimum standard [101]. UR26 (Cyber Resilience of Ships) and UR27 (Cyber resilience of on-board systems and equipment) aim to provide a set of rules that establish a common set of minimum functional and performance criteria for ships and system to ensure they are cyber resilient [102,103]. It is important to note that these rules are not applicable to all ships, only those that are contracted for construction on or after the 1 January 2024. Considering that ships can take 3 or more years to build [104] it is only realistic to expect to see these requirements implemented on ships that enter the world's fleet in 2027 or later.

UR 27 lists 31 security requirements that maritime devices must demonstrate. Of these 31, 22 are relevant to any newly designed and manufactured VDRS. In testing VDR_T only demonstrated compliance to 1 of them, with the potential if changes in the software were made to comply with a total of 16. Therefore, with only a few years before these requirements become mandatory manufacturers need to consider the impact of these rule changes when developing the next wave of devices, and how to design security into them to ensure compliance with more stringent security requirements. Many of the suggestions to follow provide some compliance with the new UR26 and UR27 requirements. For example, under requirement 4.2.4 of IACS' UR26, companies should be considering access control more broadly to digital systems. This includes the need for visitors (i.e., technicians) to

have restricted access to systems, and to be supervised during those visits. Again helping to reduce the risk of physical access by individuals to the devices. Further work would need to be completed to ensure compliance with the other performance requirements. One such piece of work could include how, through the use of a Windows OS, the VDR could run malware, antivirus and intrusion detection software, provide secure system backup options and implement secure system configuration settings (e.g., closing unused ports).

Therefore, the suggested measures above could be seen as the first, and initial steps towards better security for all maritime navigational devices, including VDRs. As both the IEC requirements and UR's highlight, these changes will only be relevant to new devices, and ships. With this in mind, the suggested measures outlined in this paper could be implemented retrospectively in older systems to help raise their minimum standard of security without the significant financial outlay required to install new VDRs within a ship's system. It is also important to reiterate that these suggestions, in isolation could lead to small improvements in security, whereas a combination of several would provide a more substantial improvement. The success of many of these suggestions hinge upon the company and manufacturer understanding the importance of the VDR, and the system that it is integrated within. A good understanding of the VDRs environment, both physically and digitally, will help to facilitate a good understanding of the risks the VDR faces, and how best to mitigate them without reducing the effectiveness of the device or overall compliance.

5. Conclusions

As discussed above many of the suggested security improvements are relatively simple and do not require a significant amount of rewording of the current standards. This review has highlighted that there are some current requirements that inhibit the inclusion of security, and are actually worsening the security of these devices. As discussed the very definition of tamper proof (See Section 3) does not fully encompass the needs of security on modern VDRs. The guidance covering VDRs provides us with a better definition that is considerate of the importance of a VDR and the security of the information it processes and stores.

This paper demonstrates that the VDRs, both new and old are vulnerable to cyber attacks, whereby valuable data can be manipulated or lost. Many of the tools needed are readily available online making it even more important that these vulnerabilities are addressed. The final sections of this paper discussed a variety of simple, yet effective measures in which the security of VDR and their data can be addressed. These mitigations can be both technical (e.g., using encryption), non-technical (e.g., the physical location of the device or access keys) and procedural (e.g., password or update policies.

The role of the VDR as evidence will become increasingly more important as the sector moves towards greater degrees of remote and autonomy. New information will need to be collected (i.e., CCTV footage [16]), and its accuracy validated, as other sources are removed (i.e., the seafarer). Without the backup of the physical eye-witness investigators will become reliant upon the stored incident data. Thus, it is within the sector's best interest to consider the security of the VDR before its data is relied upon and is considered either inaccurate, untrustworthy or not available.

Author Contributions: Conceptualization, R.H. and A.V.H.; methodology, R.H. and A.V.H.; validation, R.H., A.V.H., K.T. and K.J.; investigation, R.H., A.V.H., K.T. and K.J.; writing—original draft preparation, R.H. and A.V.H.; writing—review and editing, K.T. and K.J.; funding acquisition, K.T. and K.J. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is partly funded by the research efforts under Cyber-MAR. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Institutional Review Board Statement: The contents of this article were approved by the projects Security Advisory Board on 24 November 2022

Informed Consent Statement: Participants involved in the workshop were informed that the session was being recorded and that results would be anonymous.

Data Availability Statement: Survey data unavailable.

Acknowledgments: The authors would like to thank colleagues from the CyberSHIP lab, namely Gizem Kayisoglu, Wesley Andrews, Jordan Gurren, Juan Palbar Misas and Erlend Erstad for their invaluable support and comments on earlier drafts.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification Systems
CIA	Confidentiality, Integrity and Availability
CVSS	Common Vulnerability Scoring System
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GUI	Graphical User Interface
IACS	International Association of Classification Societies
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security Code
MAIB	Maritime Accident Investigation Branch
MFA	Multi Factor Authentication
MSC	Maritime Safety Committee
NIS	Network and Information Systems Directive
NMEA	National Maritime Electronics Association
PPT	People, Process, Technology
SOLAS	Safety of Life at Sea Convention
S-VDR	Simplified Voyage Data Recorder
UR	Unified Requirements
USCG	United States Coast Guard
VDR	Voyage Data Recorder

References

1. IMO. *Voyage Data Recorders*; International Maritime Organization: London, UK, 2022. Available online: https://www.imo.org/en/OurWork/Safety/Pages/VDR.aspx (accessed on 18 January 2023).
2. IMO. *Resolution Msc.333(90) (Adopted on 22 May 2012) Adoption of Revised Performance Standards for Shipborne Voyage Data Recorders (Vdrs)*; IMO: London, UK, 2012.
3. IACS. No. 85—Recommendations on Voyage Data Recorder, 2018. Available online: https://iacs.org.uk/download/1871#:~:text=The%20voyage%20data%20recorder%20system,recoverability%20of%20the%20recorded%20data (accessed on 18 January 2023).
4. Riviera Maritime Media. A Short History of VDR, 2009. Available online: https://www.rivieramm.com/news-content-hub/news-content-hub/a-short-history-of-vdr-48518 (accessed on 18 January 2023).
5. Joly, J. MS Estonia: New Expedition Confirms Official Accident Report, 2021. Available online: https://www.euronews.com/2021/11/18/ms-estonia-new-expedition-confirms-official-accident-report (accessed on 18 January 2023).
6. North of England P&I Association. Voyage Data Recorders (VDR): Advice for the Ship's Crew, 2015. Available online: https://www.nepia.com/media/222798/NORTH-Hot-Spots-VDR.PDF (accessed on 18 January 2023).
7. Degnarain, N. Decoding The Black Box: The 2015 US Disaster That Revolutionized Ship Crash Investigations, 2020. Available online: https://www.forbes.com/sites/nishandegnarain/2020/10/13/decoding-the-black-box-the-2015-us-disaster-that-revolutionized-ship-crash-investigations/?sh=71b75662712f (accessed on 18 January 2023).
8. National Transportation Safety Board. NTSB/MAR-17/01—Singling of the US Cargo Vessel *El Faro*, 2018. Available online: https://www.ntsb.gov/investigations/AccidentReports/Reports/SPC1801.pdf (accessed on 18 January 2023).

9. Piccinelli, M.; Gubian, P. Modern ships Voyage Data Recorders: A forensics perspective on the Costa Concordia shipwreck. *Digit. Investig.* **2013**, *10*, S41–S49. [CrossRef]
10. Tam, K.; Jones, K. Forensic Readiness within the Maritime Sector. In Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 3–4 June 2019; pp. 1–4. [CrossRef]
11. Wingrove, M. Using VDR Data to Enhance Fleet Operations and Safety, 2014. Available online: https://www.rivieramm.com/opinion/opinion/using-vdr-data-to-enhance-fleet-operations-and-safety-39120 (accessed on 18 January 2023).
12. Du, Y.; Chen, Y.; Li, X.; Schönborn, A.; Sun, Z. Data fusion and machine learning for ship fuel efficiency modeling: Part II—Voyage report data, AIS data and meteorological data. *Commun. Transp. Res.* **2022**, *2*, 100073. [CrossRef]
13. *Directive (EU) 2016/1148*; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. European Commission: Brussels, Belgium, 2016.
14. *Regulation (EU) 2016/679*; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). European Commission: Brussels, Belgium, 2016.
15. Drougkas, A. The Cyber Security Policy Framework: NIS Directive and Cyber Security in Maritime. In Proceedings of the Digital Ship Conference, Athens, Greece, 8 November 2019. Available online: https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5c056515aa4a99ba1fb7f2b1/1543857451926/14AthanasiosDrougkas_Athens18.pdf (accessed on 18 January 2023).
16. MarineLink. Danelec Unveils Synchronized VDR Data and CCTV Interface, 2022. Available online: https://www.marinelink.com/news/danelec-unveils-synchronized-vdr-data-499285 (accessed on 18 January 2023).
17. GDPR.EU. What Are the GDPR Fines? 2020. Available online: https://gdpr.eu/fines/ (accessed on 18 January 2023).
18. *Honeywell Industrial Cybersecurity USB Threat Report 2022*; Honeywell: Charlotte, NC, USA, 2022. Available online: https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Industrial-Cybersecurity-USB-Threat-Report-2022.pdf (accessed on 18 January 2023).
19. Santamarta, R. Maritime Security: Hacking into a Voyage Data Recorder (VDR), 2015. Available online: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/ (accessed on 18 January 2023).
20. IMO. *International Convention for the Safety of Life at Sea (SOLAS), 1974*; International Maritime Organization: London, UK, 2021. Available online: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx (accessed on 18 January 2023).
21. DNV-GL. EC Certificate Type Examination, 2017. Available online: https://www.scribd.com/document/440781840/VR2272B-Installation-Manual-new (accessed on 18 January 2023).
22. Furuno. VR-7000 Operator's Manual, 2019. Available online: https://www.furunousa.com/-/media/sites/furuno/document_library/documents/manuals/public_manuals/vr7000_operators_manual.pdf (accessed on 18 January 2023).
23. NetWave. NW-6000-Series Voyage Data Recorder Operator Manual, 2015. Available online: https://cirspb.ru/pdf/NW6000-00-Operator-manual-version1.3.pdf (accessed on 18 January 2023).
24. Marine, D. Type Approval Certificate—DM100 VDR G2, 2022. Available online: https://www.danelec.com/umbraco/Api/Download/media?name=DNV%20Type%20Approval%20Certificate%20DM100%20VDR%20and%20S-VDR%20G2%20with%20Float%20Free%20Capsule%20MK2.pdf&url=%2Fmedia%2Flvsnoog3%2Fdnv-type-approval-certificate-dm100-vdr-and-s-vdr-g2-with-float-free-capsule-mk2.pdf (accessed on 18 January 2023).
25. Hughes, K. Type Approval Certificate—X-VDR, 2017. Available online: https://uk.hensoldt.net/fileadmin/kh/Type-Approval-Certificates-New/X-VDR_Voyage_Data_Recorder_233.pdf (accessed on 18 January 2023).
26. *MSC.163(78)*; Performance Standards for Shipbourne Simplified Voyage Data Recorders (S-VDRs). IMO: London, UK, 2004.
27. *MSC.214(81)*; Adoption of Amendments to the Performance Standards for Shipborne Voyage Data Recorders (VDRs) (Resolution A.861(20)) and Performance Standards for Shipborne Simplified Voyage Data Recorders (S-VDRs) (Resolution MSC.163(78)). IMO: London, UK, 2006.
28. *IResolution A.694(17)*; General Requirements for Shipborne Radio Equipment Forming Part of the Global Maritime Distress and Safety System (GMDSS) and for Electronic Navigational Aids. IMO: London, UK, 1991.
29. *MSC.163(78)*; PErformance Standards for the Presentation of Navigation-Related Information on Shipborne Navigational Displays). IMO: London, UK, 2004.
30. *IEC 61996-1:2013+A1:2021*; Maritime Navigation and Radiocommunication Equipment and Systems. Shipborne Voyage Data Recorder (VDR). Performance Requirements, Methods of Testing and REQUIRED test results. International Electrotechnical Commission: Geneva, Switzerland, 2021.
31. *IEC 60945:2002*; Maritime Navigation and Radiocommunication Equipment and Systems. General Requirements. Methods of Testing and Required Test Results. International Electrotechnical Commission: Geneva, Switzerland, 2021.
32. *IEC 61162-1:2016*; Maritime Navigation and Radiocommunication Equipment and Systems. Digital Interfaces. Single Talker and Multiple listeners. International Electrotechnical Commission: Geneva, Switzerland, 2016.
33. *IEC 61162-2:1998*; Maritime Navigation and Radiocommunication Equipment and Systems. Digital Interfaces. Single Talker and Multiple Listeners, High-Speed Transmission. International Electrotechnical Commission: Geneva, Switzerland, 1998.
34. *IEC 61162-450:2018*; Maritime Navigation and Radiocommunication Equipment and Systems. Digital Interfaces. Multiple Talkers and Multiple Listeners. Ethernet Interconnection. International Electrotechnical Commission: Geneva, Switzerland, 2018.

35. *IEC 62288:2022*; Maritime Navigation and Radiocommunication Equipment and Systems—Presentation of Navigation-Related Information on Shipborne navigational Displays—General Requirements, Methods of Testing and Required Test Results. International Electrotechnical Commission: Geneva, Switzerland, 2022.
36. Cybersecurity & Infrastructure Security Agency. *Interschalt VDR G4e Path Traversal Vulnerability | CISA*; Cybersecurity & Infrastructure Security Agency: Arlington, VA, USA, 2016.
37. CVE Program. *CVE-2016-9339—Interschalt VDR G4e Path Traversal Vulnerability*; National Insitute of Standards and Technology: Gaithersburg, MD, USA, 2016.
38. Harish, A.V.; Tam, K.; Jones, K. Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack. In *Special Track: CyMAR: Cyber at Sea: Issues Concerning the Maritime Sector, along with Cyber2022*; Iaria XPS Press: Lisbon, Portugal, 2022.
39. *ISO/TS 10891*; Freight Containers. Radio Frequency Identification (RFID). Licence Plate Tag. ISO: Geneva, Switzerland, 2009.
40. *What Is the CIA Triad and Why Is It Important?*; Fortinet: Sunnyvale, CA, USA,2022.
41. *Windows Embedded Standard 7—Microsoft Lifecycle | Microsoft Learn*; Microsoft: California, CA, USA, 2022.
42. Kali Linux. Introduction: Kali linux documentation. Available online: https://www.kali.org/docs/introduction/ (accessed on 19 January 2023).
43. Lyon, G. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*; Nmap Project: Online, 2009.
44. Metasploit Penetration Testing Software, Pen Testing Security. Available online: https://www.metasploit.com/ (accessed on 18 January 2023).
45. Hak5. USB Rubber Ducky. Available online: https://shop.hak5.org/products/usb-rubber-ducky-deluxe (accessed on 03 August 2022).
46. *Keystroke*; Merriam-Webster: Springfield, MA, USA, 2022.
47. Gonzalez, A. Rubber Ducky: Learning about the Keystroke Injection | by Alejandro González | Trabe | Medium, 2022. Available online: https://medium.com/trabe/rubber-ducky-learning-about-keystroke-injection-324f462f80fa (accessed on 02 September 2022).
48. *The State of Ransomware 2022*; Sophos: New Delhi, India, 2022. Available online: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf (accessed on 18 January 2023).
49. Zdnet. All four of the world's largest shipping companies have now been hit by cyber-attacks | ZDNet, 2020. Available online: https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks (accessed on 3 August 2022).
50. Kali Linux Tools. hydra. Available online: https://www.kali.org/tools/hydra/ (accessed on 3 August 2022).
51. MalwareBytes. BadRabbit: A Closer Look at the New Version of Petya/NotPetya, 2017. Available online: https://www.malwarebytes.com/blog/news/2017/10/badrabbit-closer-look-new-version-petyanotpetya (accessed on 18 January 2023).
52. MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution, 2018. Available online: https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_psexec/ (accessed on 3 August 2022).
53. NMEA. National Marine Electronics Association—NMEA. Available online: https://www.nmea.org/nmea-0183.html (accessed on 18 January 2023).
54. MACE Times in ReFS | Forensic Investigation of Microsoft's Resilient File System (ReFS). Available online: http://resilientfilesystem.co.uk/mace-times (accessed on 3 August 2022).
55. Golitsyn, V; Paik, J-H; Robinson, P; Francioni, F; Rao, P.S., PCA Case No. 2015-28 In the matter of an arbitration-before-an arbitral tribunal constituted under annex vii to the 1982 united nations convention on the law of the sea the italian republic-v.-the republic of india-concerning-the "enrica lexie" incident permanent court of arbitration, 2020. Available online: https://pcacases.com/web/sendAttach/16500 (accessed on 18 January 2023).
56. Gardner, A. Voyage Data Recorder—Is It Ready for Use? 2021. Available online: https://britishmarine.com/news-and-advice/advice-and-notices/voyage-data-recorder-is-it-ready-for-use/ (accessed on 18 January 2023).
57. CISecurity. *Security Primer—EternalBlue*; Center for Internet Security: East Greenbush, NY, USA, 2019; p. 4722.
58. IMO. *Brief History of IMO*; International Maritime Organization: London, UK, 2022. Available online: https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx (accessed on 18 January 2023).
59. Hopcraft, R.; Martin, K.M. Effective maritime cybersecurity regulation—The case for a cyber code. *J. Indian Ocean Reg.* **2018**, *14*, 354–366. [CrossRef]
60. Morgan, J.M.; Liker, J.K. *The Toyota Product Development System—Integrating People, Process and Technology*; CRC Press: Boca Raton, FL, USA, 2006.
61. Eminağaoğlu, M.; Uçar, E.; Eren, Ş. The positive outcomes of information security awareness training in companies—A case study. *Inf. Secur. Tech. Rep.* **2009**, *14*, 223–229. [CrossRef]
62. National Institute of Standards and Technology. FIPS 140-2—Security Requirements for Cryptographic Modules, 2001. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf (accessed on 18 January 2023).
63. Abdel Hakeem, S.A.; Abd El-Gawad, M.A.; Kim, H. A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks. *IEEE Access* **2019**, *7*, 119689–119705. [CrossRef]

64. National Institute of Standards and Technology. NIST Special Publication 800-82—Guide to Industrial Control Systems (ICS) Security, 2015. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (accessed on 18 January 2023).
65. IMO. *International Ship and Port Facility Security (ISPS) Code*; International Maritime Organization: London, UK, 2021.
66. *ISO/IEC27001:2013*; Information Technology—Security Techniques— Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2013.
67. Seong, K.T.; Kim, G.H. Implementation of voyage data recording device using a digital forensics-based hash algorithm. *Int. J. Electr. Comput. Eng. (IJECE)* **2019**, *9*, 5412–5419. [CrossRef]
68. Vasu, S.; George, S.N.; Deepthi, P. An Integrity Verification System for Images using Hashing and Watermarking. In Proceedings of the 2012 International Conference on Communication Systems and Network Technologies, Rajkot, India, 11–13 May 2012. [CrossRef]
69. Vocal. DCT Transform Digital Watermarking. Available online: https://vocal.com/video/dct-transform-digital-watermarking/ (accessed on 18 January 2023).
70. Chauhan, Y.; Gupta, P.; Majumder, K. Digital Watermarking of Satellite Images. In Proceedings of the Third Indian Conference on Computer Vision, Graphics & Image Processing, Ahmadabad, India, 16–18 December 2002. [CrossRef]
71. Mojtaba Mousavi, S.; Naghsh, A.; R. Abu-Bakar, S.A. Watermarking Techniques used in Medical Images: A Survey. *J. Digit. Imaging* **2014**, *27*, 714–729. [CrossRef] [PubMed]
72. National Institute of Standards and Technology. FIPS 197—Specification for the Advanced Encryption Standard (AES), 2001. Available online: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf (accessed on 18 January 2023)
73. UK Home Office. *Investigation of Protected Electronic Information Revised Code of Practice Presented to Parliament Pursuant to Section 71(4) of the Regulation of Investigatory Powers Act 2000*; UK Home Office: London, UK, 2018.
74. Zimmermann, V.; Gerber, N. The password is dead, long live the password—A laboratory study on user perceptions of authentication schemes. *Int. J. Hum.-Comput. Stud.* **2020**, *133*, 26–44. [CrossRef]
75. Brecht, D. Password Security: Complexity vs. Length, 2021. Available online: https://resources.infosecinstitute.com/topic/password-security-complexity-vs-length/ (accessed on 18 January 2023).
76. National Cyber Security Centre. Password Policy: Updating Your Approach. 2018. Available online: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach (accessed on 18 January 2023).
77. BIMCO. The Guidelines on Cyber Security Onboard Ships v4. 2020. Available online: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed on 18 January 2023).
78. Microsoft. Download Microsoft Authenticator, 2022. Available online: https://www.microsoft.com/en-us/security/mobile-authenticator-app (accessed on 18 January 2023).
79. Summers, W.C.; Bosworth, E. Password Policy: The Good, the Bad, and the Ugly. In *Proceedings of the Winter International Synposium on Information and Communication Technologies, WISICT '04, Cancun Mexico, 5–8 January 2004*; Trinity College Dublin: Dublin, Ireland, 2004; pp. 1–6.
80. National Institute of Standards and Technology. NIST Special Publication 800-63B—Digital Identity Guidelines, 2017. Available online: https://pages.nist.gov/800-63-3/sp800-63b.html (accessed on 18 January 2023).
81. *ISO/IEC27002:2017*; Information Technology—Security Techniques—Code of practice for information security controls. ISO: Geneva, Switzerland, 2017.
82. Huang, D.L.; Patrick Rau, P.L.; Salvendy, G.; Gao, F.; Zhou, J. Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int. J. Hum.-Comput. Stud.* **2011**, *69*, 870–883. [CrossRef]
83. Ambinder, M. 2 White House Movie Tropes That Don't Make Sense, 2015. Available online: https://theweek.com/articles/462339/2-white-house-movie-tropes-that-dont-make-sense (accessed on 18 Janaury 2023).
84. KeySure. KeySure Key Control Product, 2022. Available online: https://www.keysure.net/ (accessed on 18 January 2023).
85. CashStash. CashStash, 2013. Available online: https://www.thingiverse.com/thing:110897 (accessed on 18 January 2023).
86. Cavusoglu, H.; Cavusoglu, H.; Zhang, J. Security Patch Management: Share the Burden or Share the Damage? *Manag. Sci.* **2008**, *54*, 657–670. [CrossRef]
87. Microsoft. Windows 10 Update Servicing Cadence, 2018. Available online: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-10-update-servicing-cadence/ba-p/222376 (accessed on 18 January 2023).
88. *IEC 62443-3-2:2020* Security for Industrial Automation and Control Systems. International Electrotechnical Commission: London, UK, 2020.
89. *NIST Special Publication 800-61—Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [CrossRef]
90. *ISO/IEC27035-3:2020*; Information Technology—Information Security Incident Management. ISO: Geneva, Switzerland, 2020.
91. *Cyber Strategic Outlook Aug 2021*; US Coast Guard: Washington, DC, USA, 2021.
92. US Coast Guard. CVC-WI-027(1)—Vessel Cyber Risk Management Work Instruction. 2020. Available online: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-027(series).pdf (accessed on 18 January 2023).
93. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity—Version 1.1. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 18 January 2023).

94. *The 'Enrica Lexie' Incident (Italy v. India)*; Permanent Court of Arbitration: The Hague, The Netherlands, 2020.
95. *Voyage Data Recorder Vr-5000 (Serial Number 1001 or Greater)*; Furuno: Hyogo, Japan, 2005.
96. Hodgkinson, S. The Voyage Data Recorder (VDR), 2022. Available online: https://www.westpandi.com/publications/news/april-2022/the-voyage-data-recorder-(vdr)/ (accessed on 18 Janaury 2023).
97. Hopcraft, R. Developing Maritime Digital Competencies. *IEEE Commun. Stand. Mag.* **2021**, *5*, 12–18. [CrossRef]
98. *Msc.1/Circ.1222/Rev.1)—Guidelines on Annual Testing of Voyage Data Recorders (Vdr) And Simplified Voyage Data Recorders (S-Vdr)*; IMO: London, UK, 2019.
99. *IEC63154:2021*; Maritime Navigation and Radiocommunication Equipment and Systems—Cybersecurity—General Requirements, Methods of Testing and Required Test Results. IEC: London, UK, 2021.
100. IACS. *About IACS*; International Association of Classification Societies: London, UK, 2022. Available online: https://iacs.org.uk/about/ (accessed on 18 January 2023).
101. IACS. *Unified Requirements*; International Association of Classification Societies: London, UK, 2022. Available online: https://iacs.org.uk/publications/unified-requirements/ (accessed on 18 January 2023).
102. IMO. *E26—Cyber Resilience of Ships*; International Association of Classification Societies: London, UK, 2022. Available online: https://iacs.org.uk/download/14104 (accessed on 18 January 2023).
103. IACS. *E27—Cyber Resilience of On-board Systems and Equipment*; International Association of Classification Societies: London, UK, 2022. Available online: https://iacs.org.uk/download/14105 (accessed on 18 January 2023).
104. Chokshi, N. How Giant Ships Are Built, 2020. Available online: https://www.nytimes.com/interactive/2020/06/17/business/economy/how-container-ships-are-built.html (accessed on 18 January 2023).