Raising the Standard of Maritime Voyage Data Recorder Security

Avanthika Vineetha Harish

Rory Hopcraft

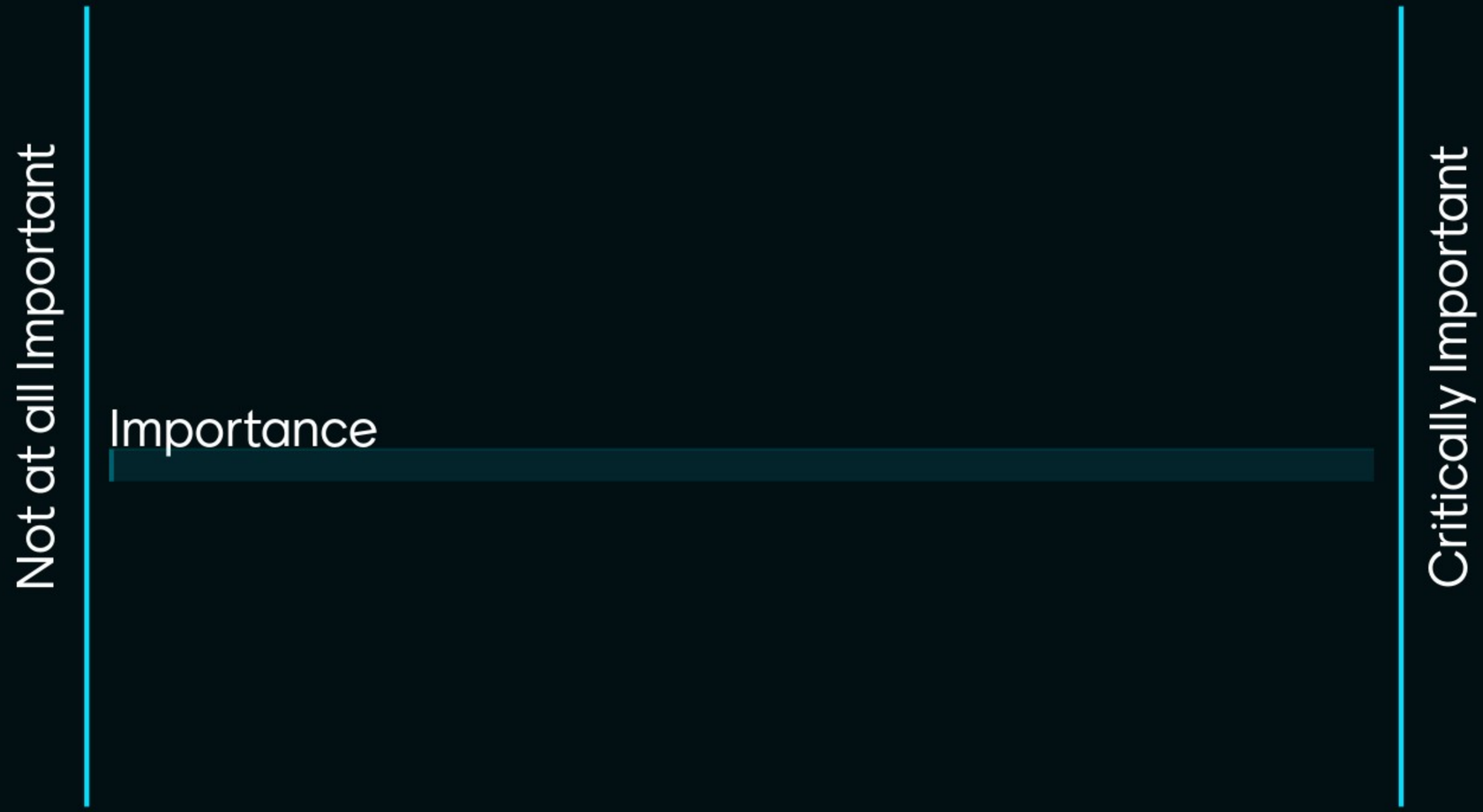
Kimberly Tam

Kevin Jones

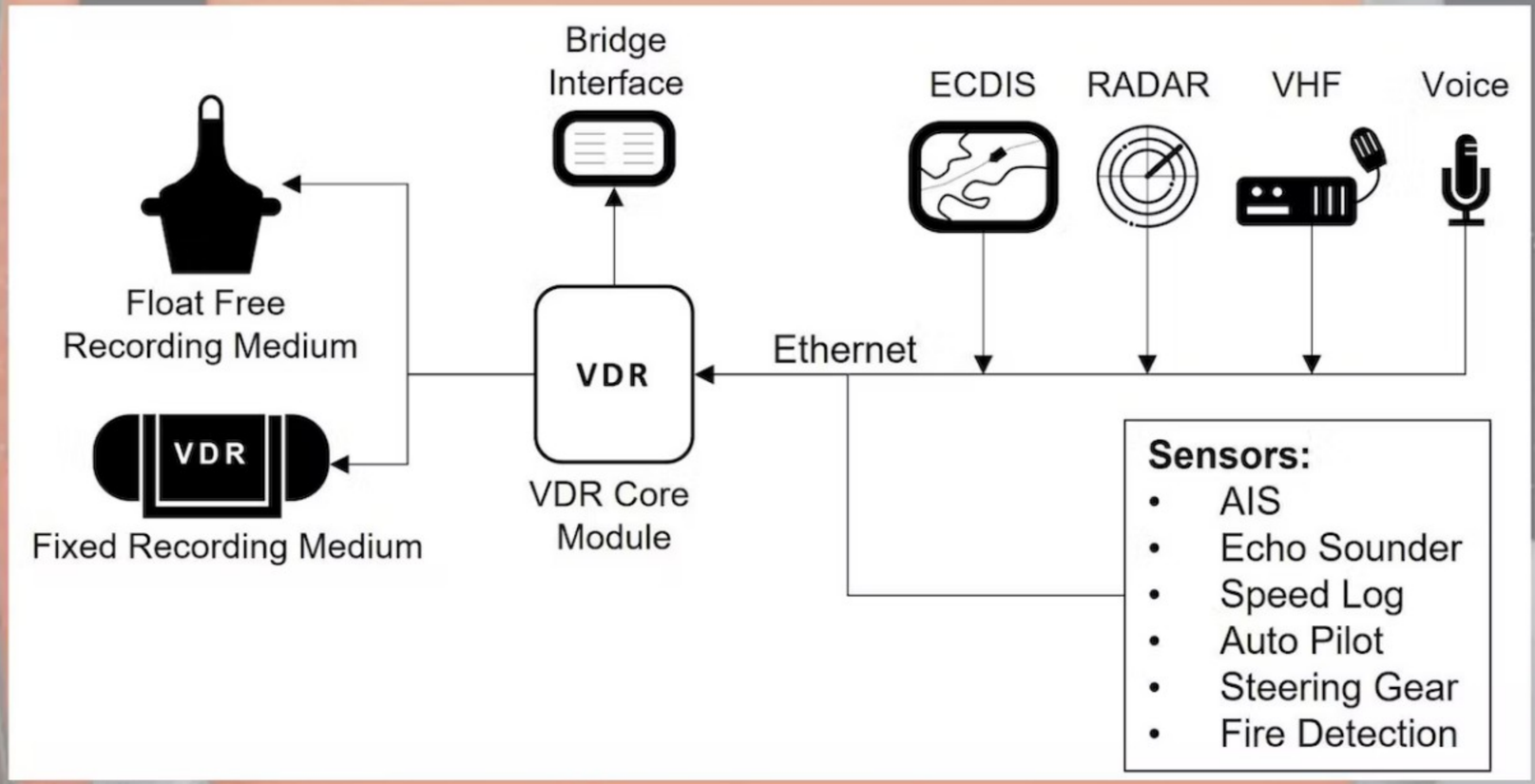
Outline

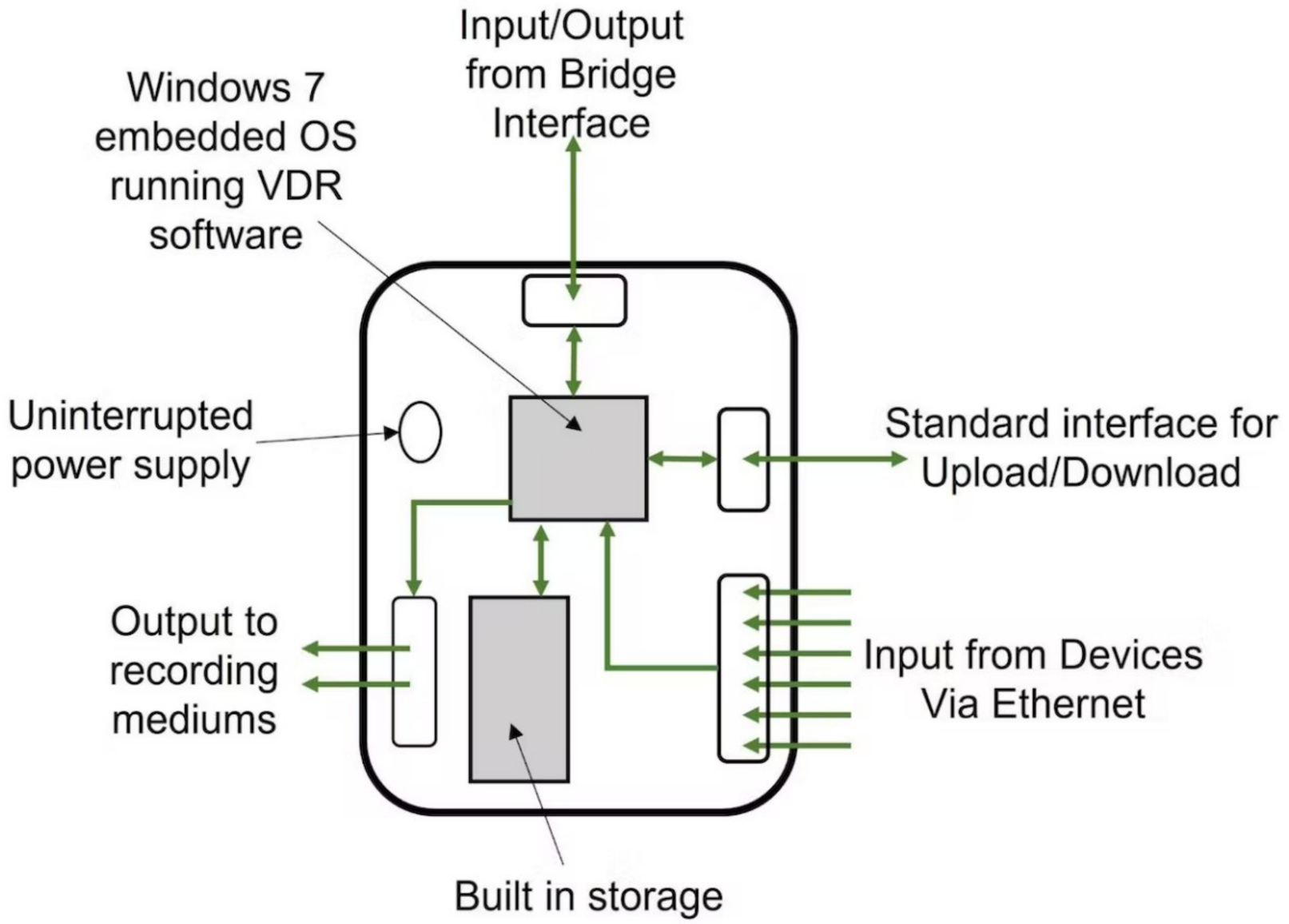
- What is the VDR, and why is it important?
- VDR Standards and a lack of security?
- Attacking the VDR
- Recommendations to improve the security of VDRs
- Conclusions

How Important Do You Think the VDR Is?



Voyage Data Recorder




Input/Output
from Bridge
Interface
Windows 7
embedded OS
running VDR
software
Uninterrupted
power supply
Standard interface for
Upload/Download
Output to
recording
mediums
Input from Devices
Via Ethernet
Built in storage

Overview of standards

Manufacturer	AMI Marine	Furuno	NetWave Systems
Device	X2 VDR	VR-7000 VDR	NW-6000 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)
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 (Annex K & M)	IEC 61996-1:2013 IEC 60068-2-27:1987 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

IMO Documents – Security Requirements?

IMO Regulations	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
	MSC.163(78)	- Performance Standards for Shipborne Simplified Voyage Data Recorders (S-VDRs)
	MSC.191(79)	- Performance Standards for the Presentation of Navigation-Related Information on Shipborne Navigational Displays
	MSC.333(90)	- Adoption of Revised Performance Standards for Shipborne Voyage Data Recorders (VDRs)

IEC Standards – Security Requirements?

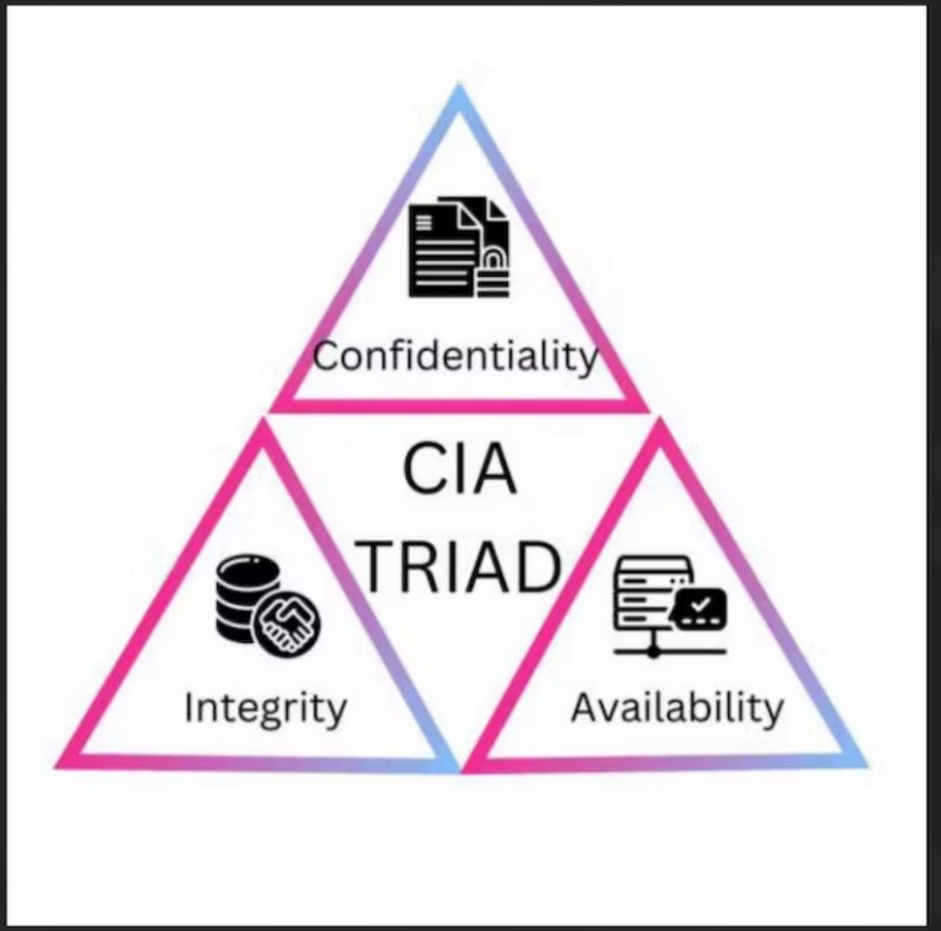
IEC Standards		
	IEC 60945:2002	- Maritime navigation and radio communication equipment and systems. General requirements. Methods of testing and required test results
	IEC 62288:2014	- Maritime navigation and radiocommunication equipment and systems. Presentation of navigation-related information on shipborne navigational displays. General requirements, methods of testing and required test results
	IEC 61996-1:2013	- Maritime navigation and radiocommunication equipment and systems. Shipborne voyage data recorder (VDR). Performance requirements, methods of testing and required test results
	IEC 61162-1	- Maritime navigation and radiocommunication equipment and systems. Digital interfaces. Single talker and multiple listeners
	IEC 61162-2	- Maritime navigation and radiocommunication equipment and systems. Digital interfaces. Single talker and multiple listeners, high-speed transmission
	IEC 61162-450	- Maritime navigation and radiocommunication equipment and systems. Digital interfaces. Multiple talkers and multiple listeners. Ethernet interconnection

Information security and CIA

Confidentiality – ensuring data is not available to unauthorised individuals e.g. accessing passwords

Integrity – ensuring recorded data is accurate as it is relied upon for maritime investigations

Availability – ensuring data is accessible when required e.g. recordings not being able to be disrupted or deleted



All icons are from Nounproject

Rank Elements of CIA in order of Importance

1st | Confidentiality

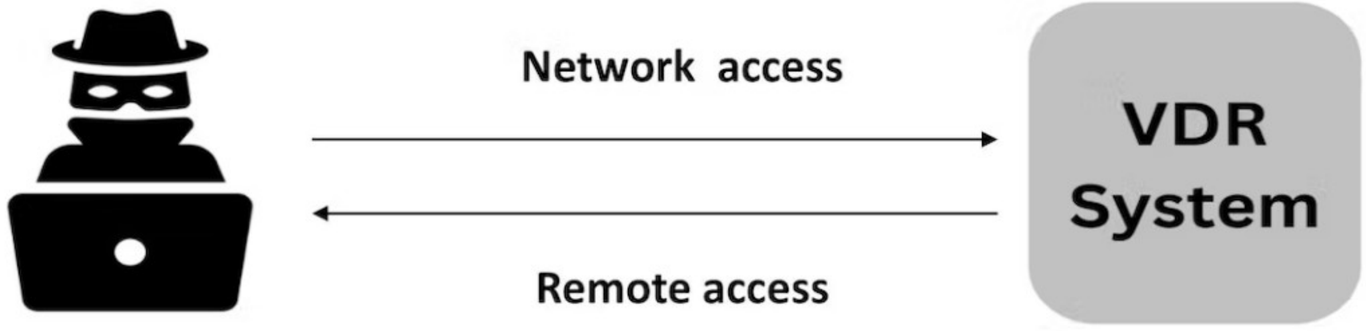
2nd | Integrity

3rd | Availability

Confidentiality

Attack vector / tools

- NMAP – Network scanner
- Metasploit – Pen-testing tool
- Eternal Romance exploit



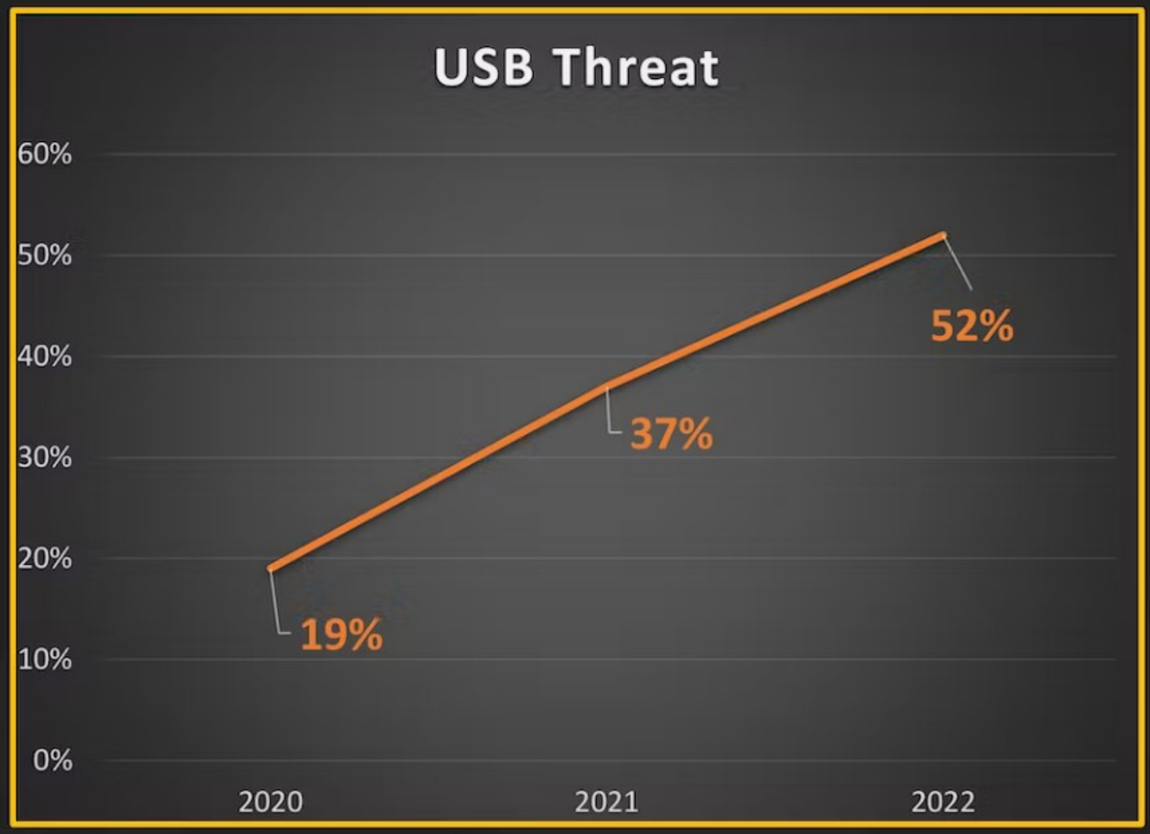
Findings / Consequences

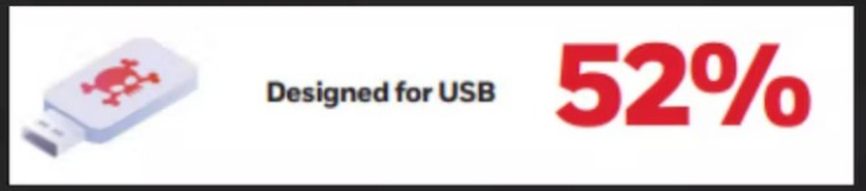
- Passwords of 5 user accounts
- Remote control of VDR
- Access to files and logs
- Download / upload data

All icons are from Nounproject

USB – Attack Vector

USB Rubber ducky



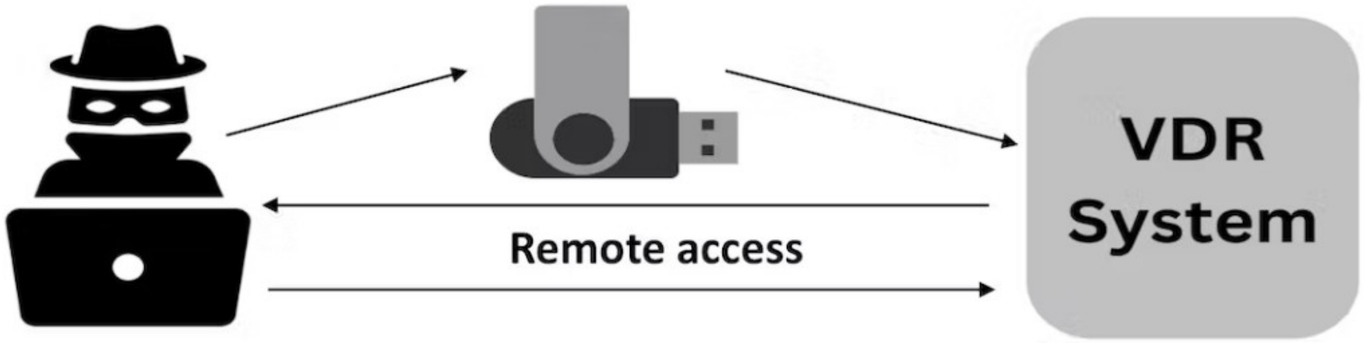


Source:
https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Industrial-Cybersecurity-USB-Threat-Report-2022.pdf

Integrity

Attack vector / tools

- USB Rubber ducky
- Metasploit – Pen-testing tool
- Reverse shell payload



Findings / Consequences

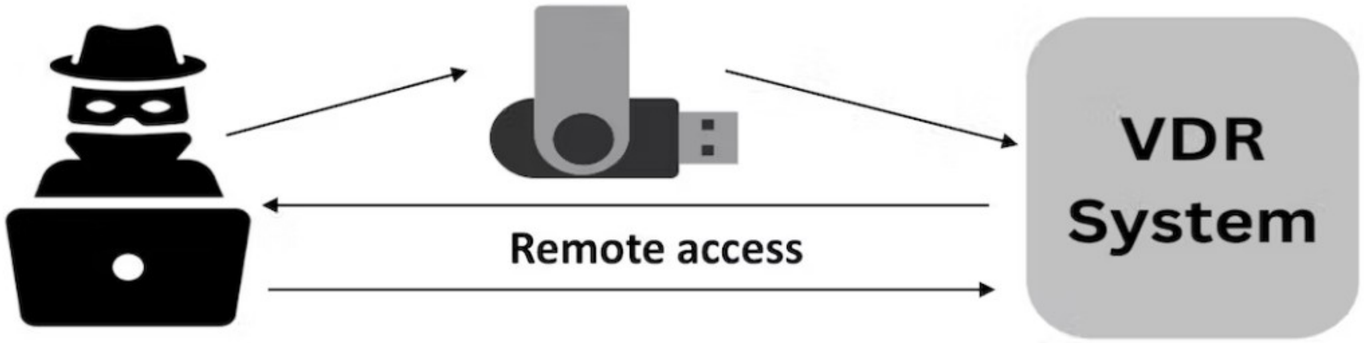
- Access to files and folders
- Tampering of archived NMEA zip data
- VDR data altered, hiding the trace

All icons are from Nounproject

Availability

Attack vector / tools

- USB Rubber ducky
- Metasploit – Pen-testing tool
- Ransomware simulator
- Eternal Blue exploit



Findings / Consequences

- Files encrypted; not available
- VDR crashes; system not available
- Data tampered through reverse shell; data not available
- Hard drive erasure; data not available

All icons are from Nounproject

Need to Improve the Standards?

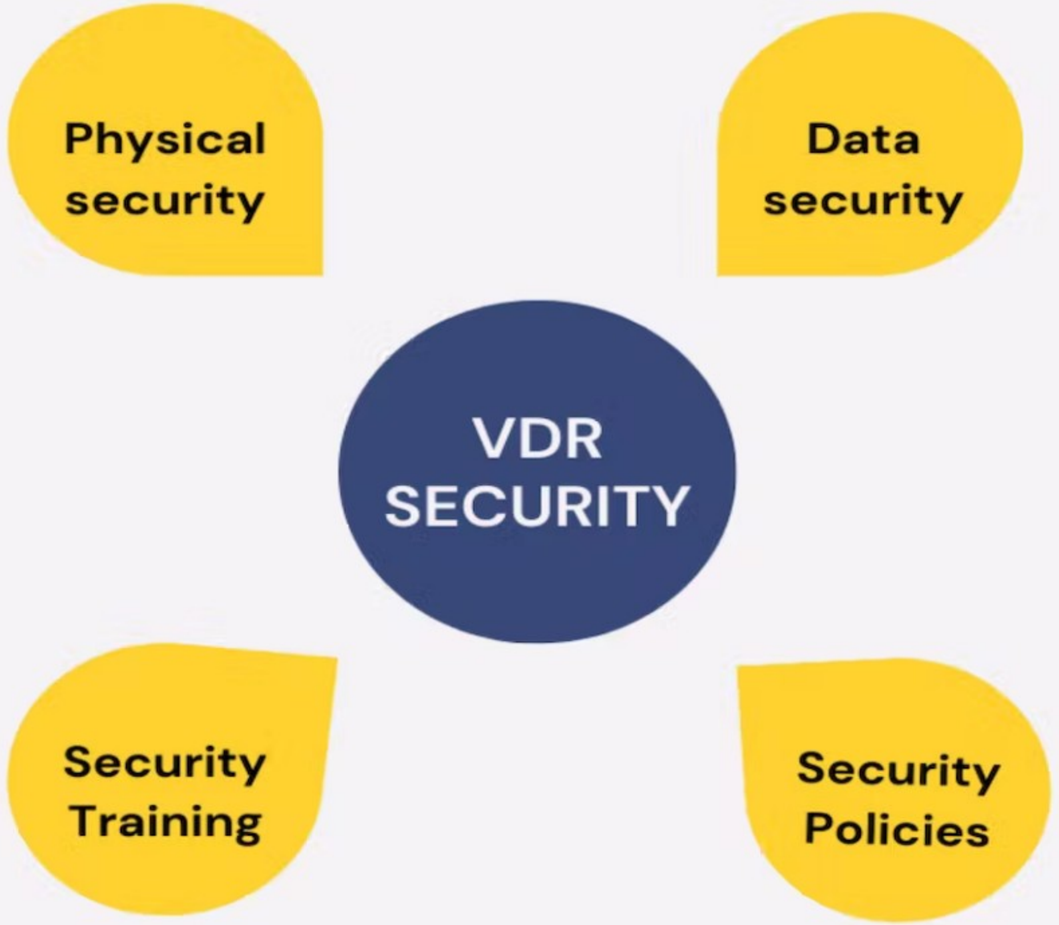
- Current standards leave VDRs open to attack
  - Ease of access requirements
  - Access to data interface

- Definition of tamper-proof does not cover information security

"secure against a physical or electronically manipulated change or deletion of recorded data"

Source: MSC.333(90)

Components of VDR Security



Rank the Importance the Components of VDR Security

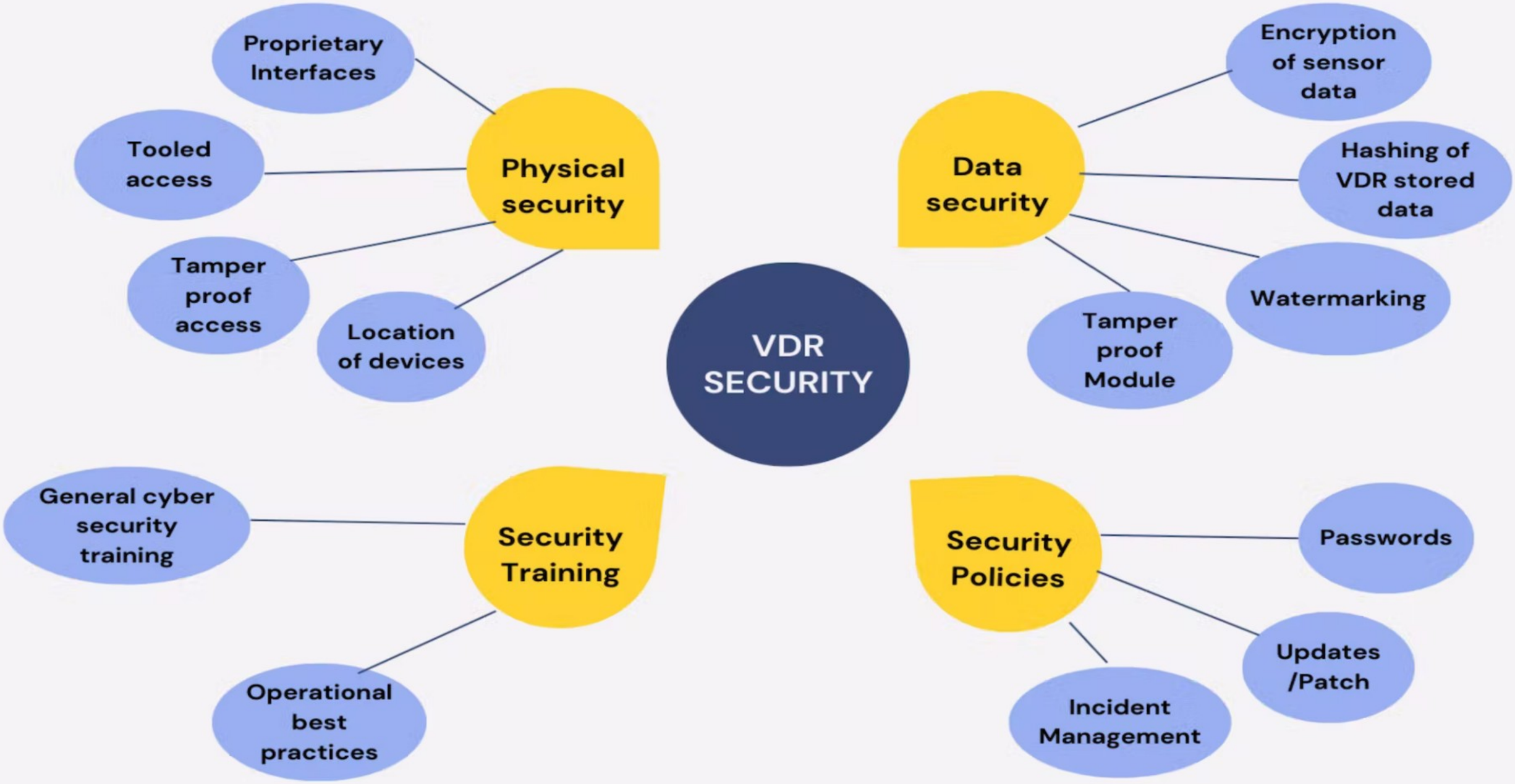
1st | Physical Security

2nd | Data Security

3rd | Security Training

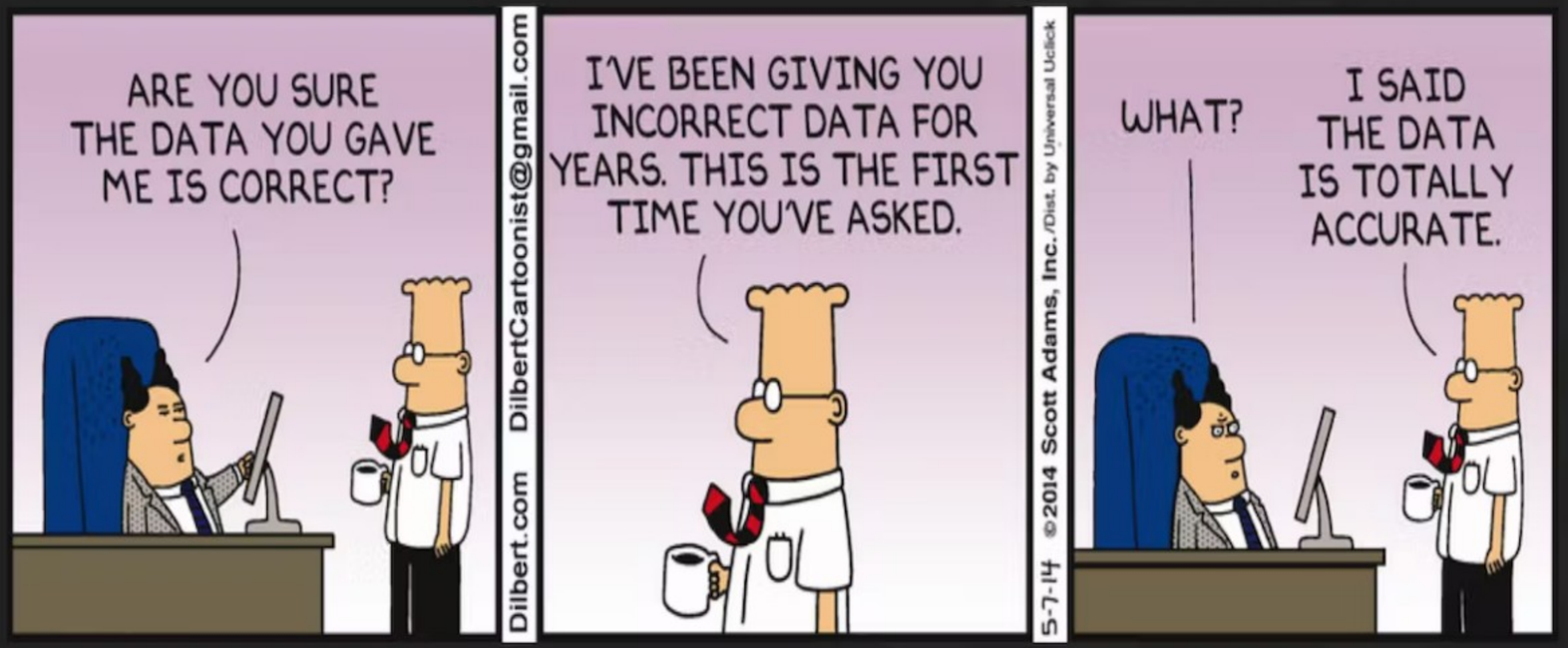
4th | Security Policy

Anything we have missed? Anything that wouldn't work? Anything that works? General Thoughts...


VDR SECURITY
Physical security
Proprietary Interfaces
Tooled access
Tamper proof access
Location of devices
Data security
Encryption of sensor data
Hashing of VDR stored data
Watermarking
Tamper proof Module
Security Training
General cyber security training
Operational best practices
Security Policies
Passwords
Updates /Patch
Incident Management

Summary

- Information security is a vital part of modern maritime operations
- Current performance requirements lack information security aspect
- A range of measures are available that could improve security



This paper is a 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.