SOUTH WEST PACIFIC REGIONAL HYDROGRAPHIC COMMISSION

MARITIME CYBERSECURITY PRIMER

Lt Cdr Nelson McMillan RN
UK Maritime Domain Awareness International Liaison Officer
14 February 2023

Scope

RISKS

What cyber risks exist in the maritime domain?

CASE STUDIES

Including an ECDIS related hit in 2022

FOLLOW-ON POINTS

5 things hydrographers need to know about cybersecurity

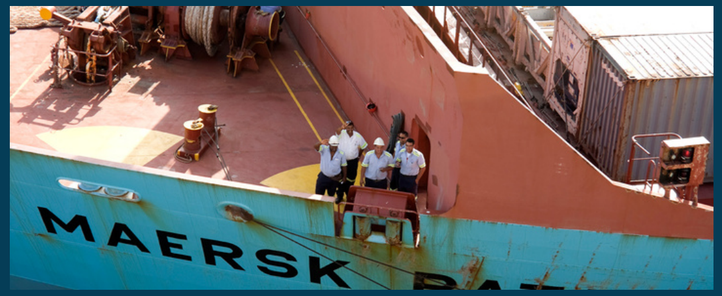
WHAT CYBER RISKS EXIST IN THE MARITIME DOMAIN?

DIGITAL TOOLS	OLD & COMPLEX INFRA-STRUCTURE	CYBER STAFF - A RARE COMMODITY	STRATEGY & PLANS
A growing reliance on these from merchant and military mariners	Understanding and pinpointing threats while identifying digital vulnerabilities	Lack or absence of IT and cybersecurity literate staff onboard ships and ashore	Business recovery plans not tested with ownership often unclear

CASE STUDIES

JNPT 2022

Jawaharlal Nehru Port Container Terminal (JNPT), India, Ransomware



MAERSK 2017

NotPetya malware designed to spread on computer information system networks

ECDIS 2022

Crew members unknowingly use infected USB stick for chart updates

5 THINGS HYDROGRAPHERS NEED TO KNOW ABOUT CYBERSECURITY

Threat Landscape

Cybersecurity is about more than protecting data

Leadership Focus

Executives must focus on risk, reputation, and business continuity

Knowledge

Senior hydrographic leaders must be knowledgable participants

Defence in Depth

A layered technology approach and human oversight is needed

Mindset

Cybersecurity is an organisational problem, not just technical

Conclusion

UNDERSTAND

Hydrographic vulnerabilities & priorities

STRESS-TEST

Your cybersecurity strategy

INVEST

In cybsecurity training

COLLABORATE

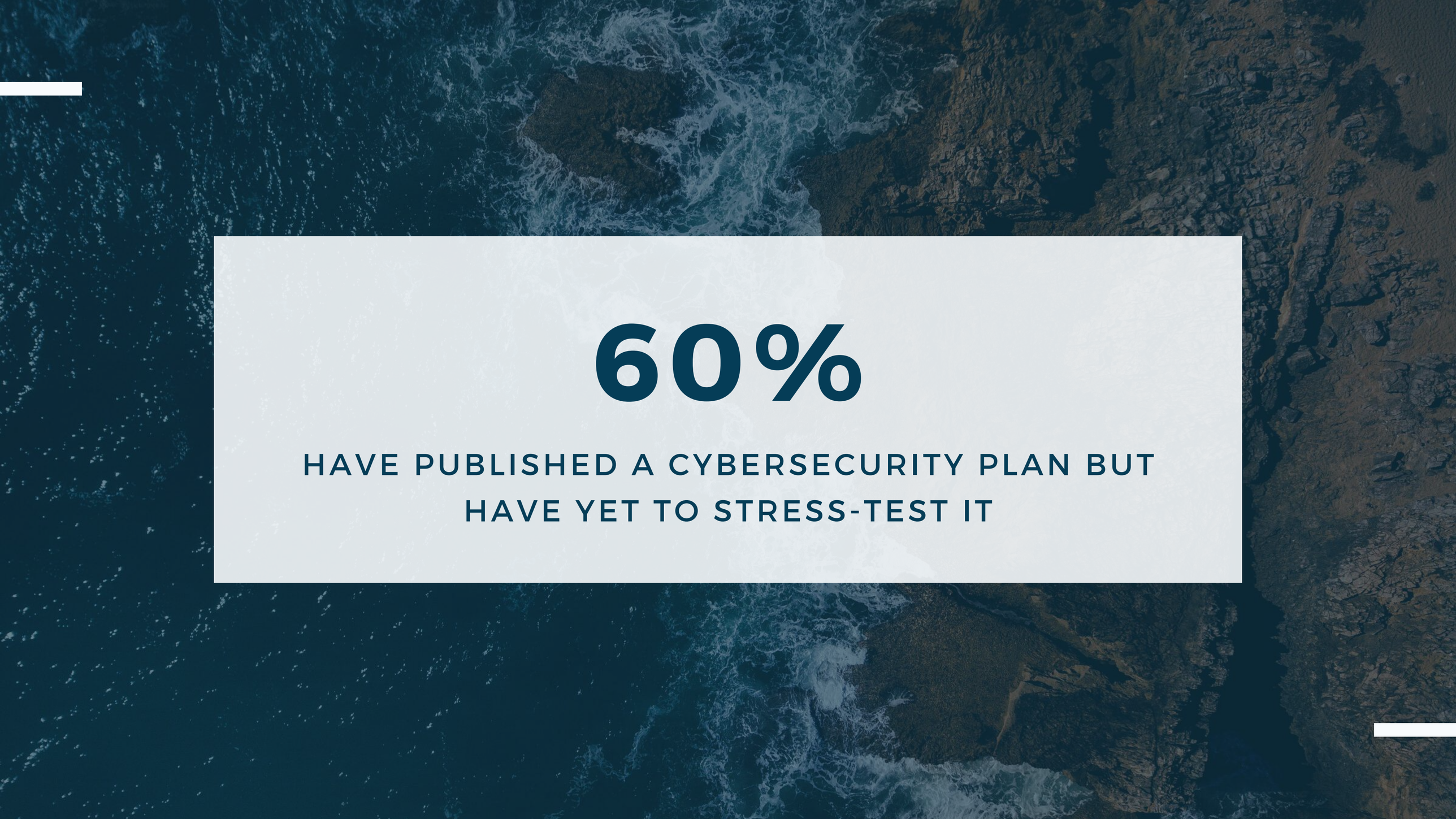
At local, national, and regional levels

68%

DISCUSS CYBERSECURITY AT SENIOR LEVEL REGULARLY OR CONSTANTLY

9%

DO NOT DISCUSS CYBERSECURITY AT BOARD LEVEL IN FORTUNE 500 COMPANIES



60%

HAVE PUBLISHED A CYBERSECURITY PLAN BUT HAVE YET TO STRESS-TEST IT

Cyber questions senior hydrographers need to ask

1. What are our most important assets and how are we protecting them?

2. What are the layers of protection we have put in place?

3. How do we know if we've been breached? How do we detect it?

4. What are our response plans in the event of an incident?

5. What is our role, at hydrographic office board level, in an incident?

6. What are our business recovery plans in the event of a cyber incident?

7. Is our cybersecurity investment enough?