REMOTE ACCESS ON VESSELS

FOCUS ON CYBERSECURITY

Fotis Tsitsirigkos , Fleet IT Manager @ Euronav

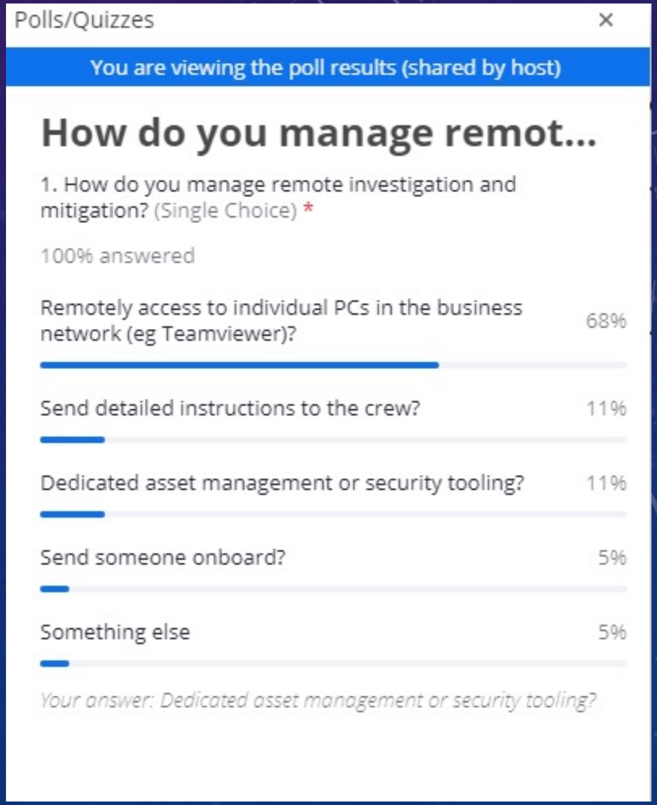
COVID-19 RAISED THE DEMAND FOR REMOTE ACCESS

- Remote Inspections / Audits
- Remote Briefing / Debriefing
- VC with HQ
- Provide Access to Business Systems on Board for
  - Training
  - Support
- Remote Maintenance of
  - IT Systems
  - Third Party Software Maintenance / Configuration
  - OT systems
  - Sat Systems
- New Systems Sending Data Remotely
  - Ballast Water Treatment
  - Vibration Analysis
  - Engine Performance Data

Third Party Remote Access

REMOTE PRIVILEGED ACCESS IS EVERYWHERE

- Over 96% of organizations rely on Third Party Vendors to access critical systems.
- 59% use up to 100 third party vendor users
- 41% use over 100 third party vendor users.



You are viewing the poll results (shared by host)

How do you manage remot...

1. How do you manage remote investigation and mitigation? (Single Choice) *

100% answered

Remotely access to individual PCs in the business network (eg Teamviewer)? 68%

Send detailed instructions to the crew? 11%

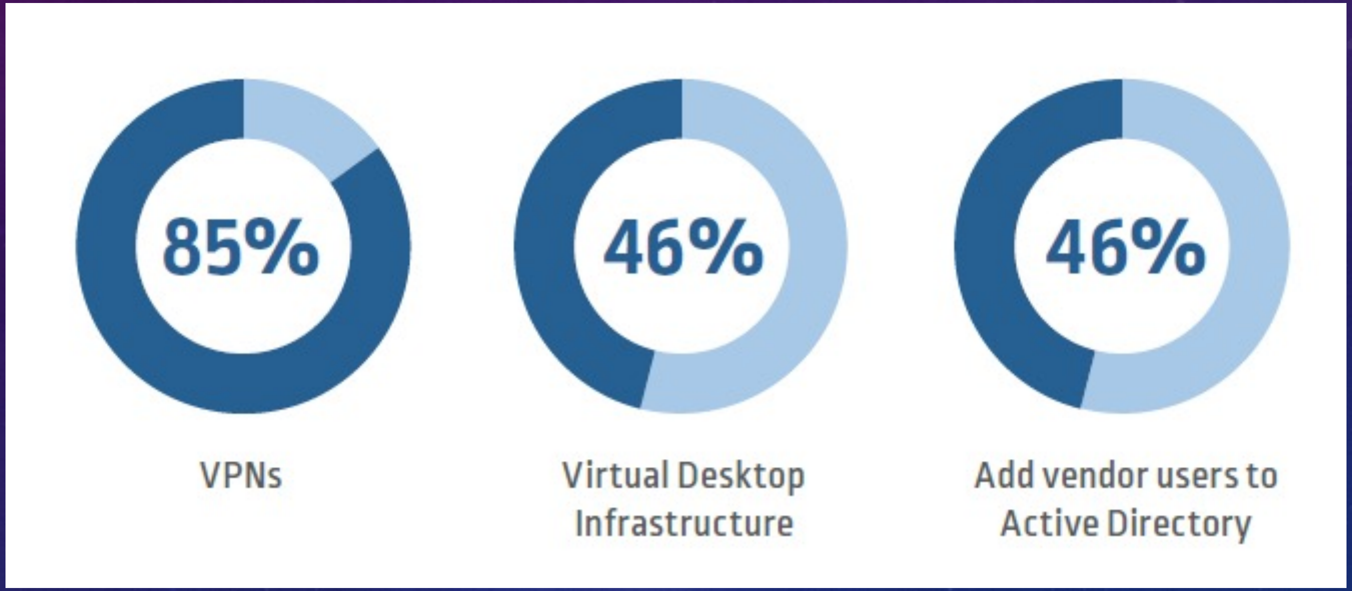
Dedicated asset management or security tooling? 11%

Send someone onboard? 5%

Something else 5%

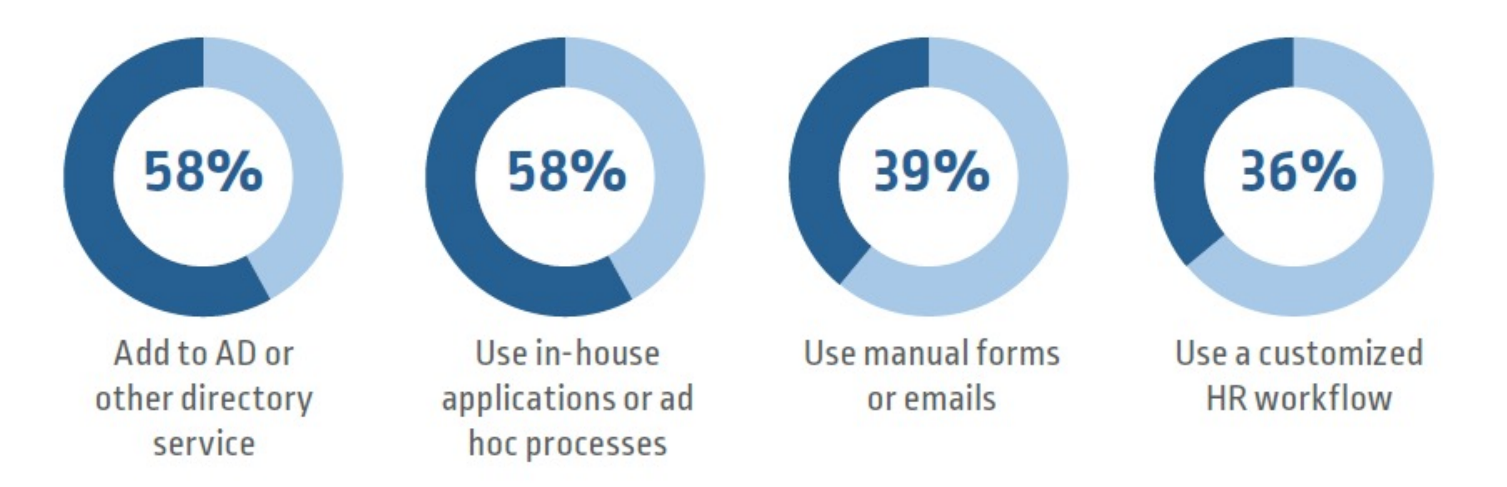
Your answer: Dedicated asset management or security tooling?

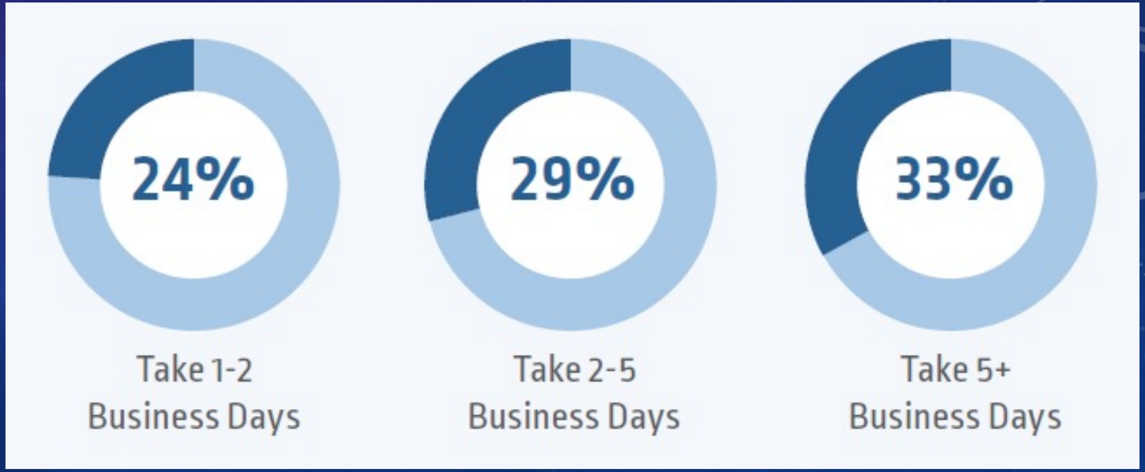
HOW IS REMOTE ACCESS GIVEN NOW?



- 1/3 of have not implemented basic MFA for remote vendors

PROVISIONING/DEPROVISIONING





IS REMOTE ACCESS ON VESSELS A TECHNICAL CHALLENGE?

- Technical
    - Cyber Security Systems and Parameters
- Non Technical
    - Internal Policies / Procedures
    - Third Party Cyber Security Level
        - Policies / Procedures
        - Systems
        - Third Party Evaluation / Liabilities

CYBER SECURITY CHALLENGES

- JUST AS CHALLENGING IS LACK OF VISIBILITY: WHO IS DOING WHAT, WHEN?
- Third Party Requirements
  - Multiple VC Platforms
  - Multiple VPN
- Third Party Cyber Evaluation
- Remote Access into Multiple Network Segments
- Remote Access into Isolated Systems
- Security vs Performance

THINK IF YOU CAN ANSWER THE BELLOW QUESTIONS

- How many vendors are accessing your network and systems?
- Which individuals within a third-party organization are accessing those resources?
- Are the individuals accessing your network still employed by the third-party vendor?
- What information do your third-party vendors need to access on your network and systems?
- Can you restrict network access to only the information required — or do you grant access to all of your systems?
- When did your third parties access your network — and what have they accessed, modified, or deleted?
- Can you see when your third-party vendors accessed your network and systems — and what information they accessed, modified, or deleted

FRONT DOOR LOCKED, WINDOWS OPEN: AN ANALOGY

While many companies and their IT personnel focus on secure internal company access, these same businesses may not have a secure third-party remote access solution.

- advanced remote (especialy for third-party) access platform
- internal risk training
- robust vendor security policies

BEST PRACTICES - GENERAL

- **Create a realistic third-party access security policy**
  - Protect your most valuable data by considering how it may be vulnerable and simple steps that can be taken to mitigate risk. Look at different options to protect your organization. As organizations continue to struggle over where responsibility lies and who is liable in the event of a data breach, taking a holistic approach is critical in protecting your organization.
- **Prepare for an attack from multiple vectors**
  - A great place to start is to catalog the points of entry into your network and prioritize which present the greatest security vulnerability. Remember, threats can come both internally and externally

BEST PRACTICES - PAM

- Introduce a PAM (Privilege Access Management) system including functionality as
  - Full and Detailed Logging of Activities
  - Support two factor authentication
  - Support of Multiple Protocols (RDP, SSH)
  - Not sensitive to low speed – high latency communications
  - Centralized Management
  - Workflow Support for Approval of Access Requests
    - Business Units shall be responsible for approving Third-Party Remote Access

BEST PRACTICES - VPN

- Optimize VPN Performance
  - For low speed – high latency communications
  - Balance between security and performance
- Support VPN Tokens
- Prefer SSL-VPN for better performance

BEST PRACTICES - NETWORK

- Further Network Segregation
  - Business / Crew Segregation only is not enough any more
- Use of VLAN and Firewall
    - Number of VLANs shall be same with Number of Function Served
    - Ideally Number of VLAN shall be same with Number of Systems
- Restrict / Limit Outbound Traffic
- Utilize Jump Host / Box Approach

COVID-19 AS AN OPPORTUNITY

- To develop / extend remote access to vessels
- To Request more services by satellite service suppliers
- To invest in required technologies and services
- Level-up the Cyber Security Awareness