2016 cyber security survey in association with BIMCO

IHS Markit and BIMCO launched the maritime cyber security survey on 22 July. The survey, which ran for four weeks, was promoted on social media and via email. More than 300 industry players responded. Of the 300 respondents, 65 had been a victim of a cyber attack. Here are some of the highlights of the insights gathered from respondents to the maritime cyber security survey.

Who responded?
- Shipowner
- Shipmanager
- Trade organisation
- Regulator
- Port authority
- Maritime services provider
- Equipment provider
- Shipyard
- Other

What is in place to protect against cyber attack?
- Intrusion detection/prevention system
- Review of log files
- Firewalls
- Physical segregation of networks
- Virtual segregation of network nodes
- Best practice protocols
- Independent cyber security consultants
- Other

Have you been a victim of cyber attack?
- Yes
- No
- No responses

Were protection strategies in place?
- Yes
- No
- No responses

What was the nature of the attack?
- Malware
- Phishing
- Spear Phishing
- Application attack
- Brute force
- Denial of service
- Network of protocol attack
- Man in the middle
- Theft of credentials
- Known vulnerability
- Other

What was the extent of the attack?
- Loss of corporate data
- Financial loss
- IT system functionality
- Shipborne systems functionality

Which shipborne systems are most vulnerable?
- ECDIS
- VDR
- IBS
- Positioning system
- BNWAS
- GMSS
- Cargo control systems
- Engine control and monitoring systems
- Other

Malware 77%
Phishing 57%
Spear Phishing 23%
Application attack 9%
Brute force 13%
Denial of service 18%
Network of protocol attack 14%
Man in the middle 4%
Thief of credentials 25%
Known vulnerability 7%
Other 9%