IHS Markit™

Maritime Cyber Survey 2018 - the results

Not for onward distribution

Embargoed until 14/09/18

Fairplay | BIMCO | ABS Advanced Solutions

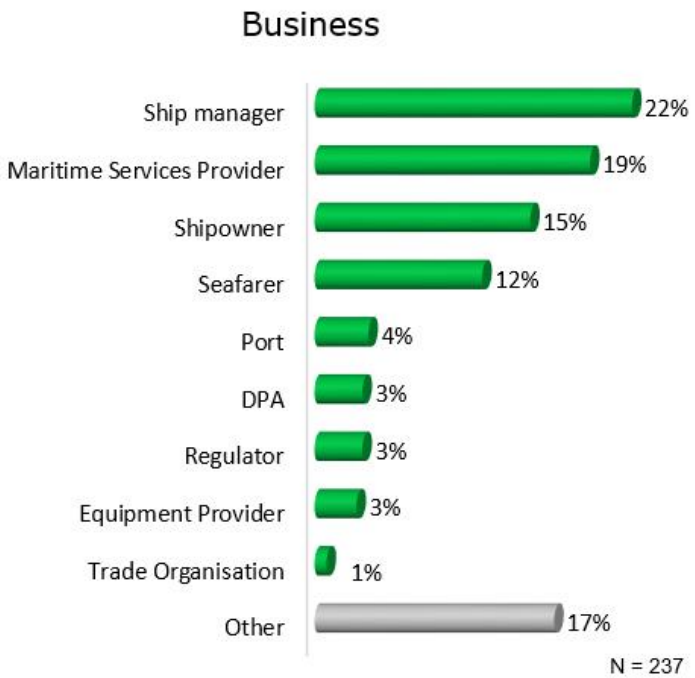
Fairplay | **Insight**

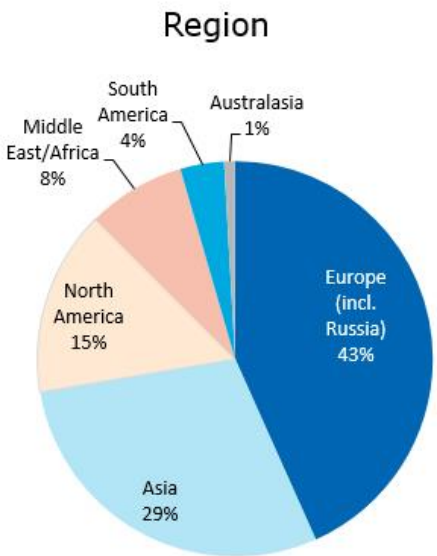
Overview

- In the wake of recent high profile cyber incidents, Fairplay and BIMCO jointly organised the third annual Maritime Cyber Security Survey to examine how the maritime industry is handling digital protection.
- Recent high-profile incidents (Maersk, Cosco, BW Group and Clarksons) have raised awareness of the risks facing maritime companies and increased the need for the sector to take the issue seriously.
- More than a fifth of respondents acknowledged that they had been the victim of an incident, with 72% of these respondents mentioning that their own company was a victim of cyber crime related incident in the last 12 months.
- Phishing (49%) and Malware-like viruses, Trojans and worms (44%) were the most common form of incident faced by respondents, mostly leading to service disruption (49%) and system downtime (44%).
- The online survey was launched in June 2018 and was promoted via bespoke emails, social media and marketing collateral in Fairplay newsletters and print.

Who responded

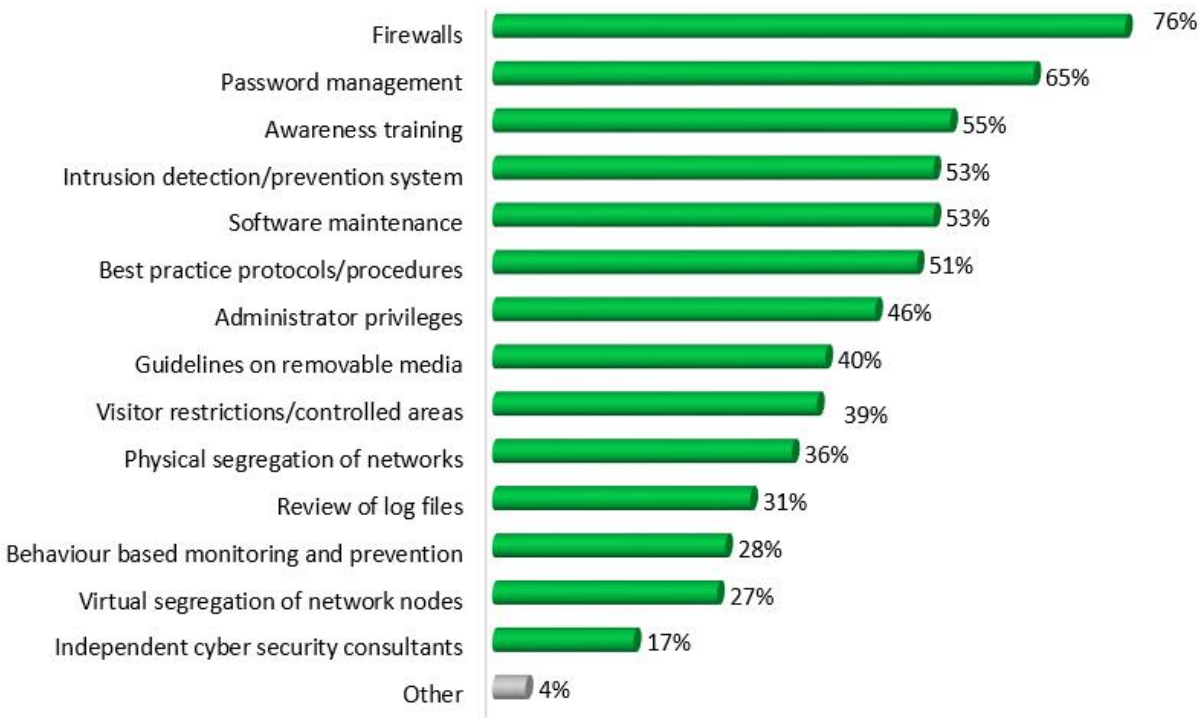
More than 350 individuals took the survey, with fully complete entries totalling 237.



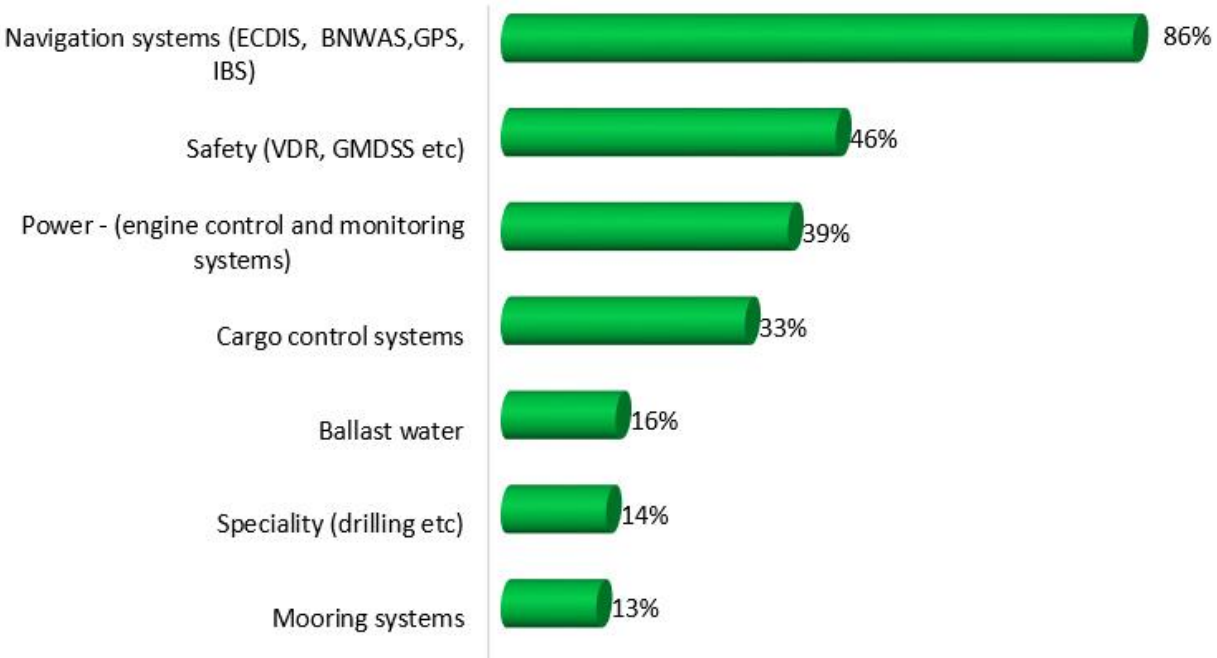


Industry overview: maritime's response to the cyber threat

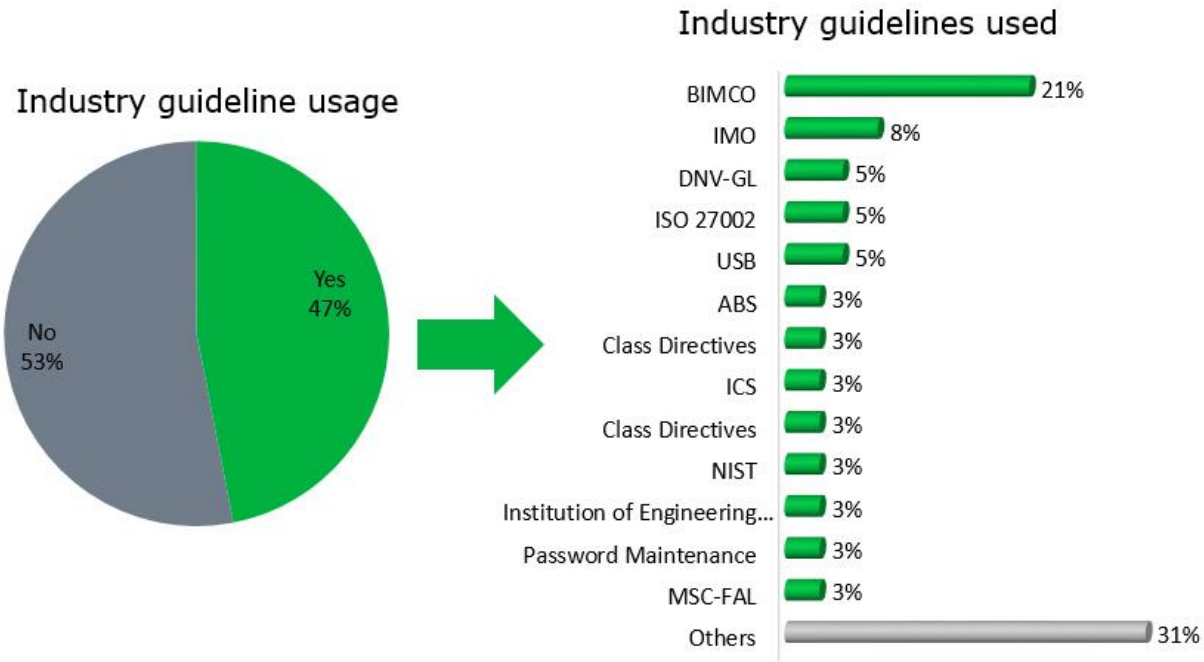
Measures being used for protection



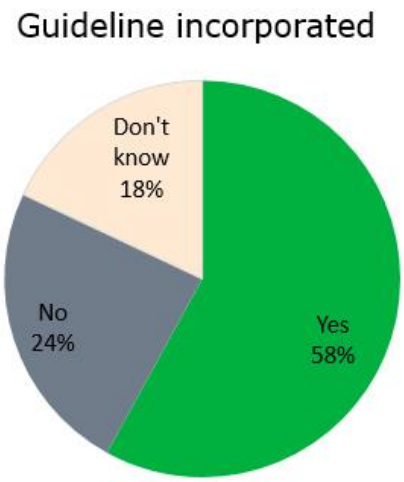
Areas perceived as most vulnerable to attack



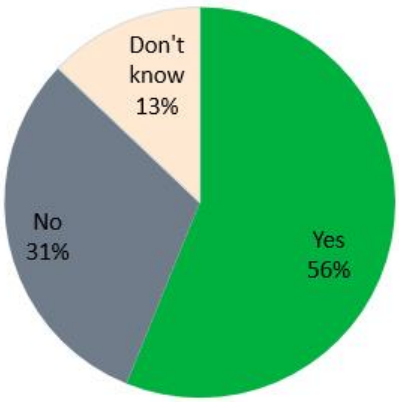
Take up of industry guidelines



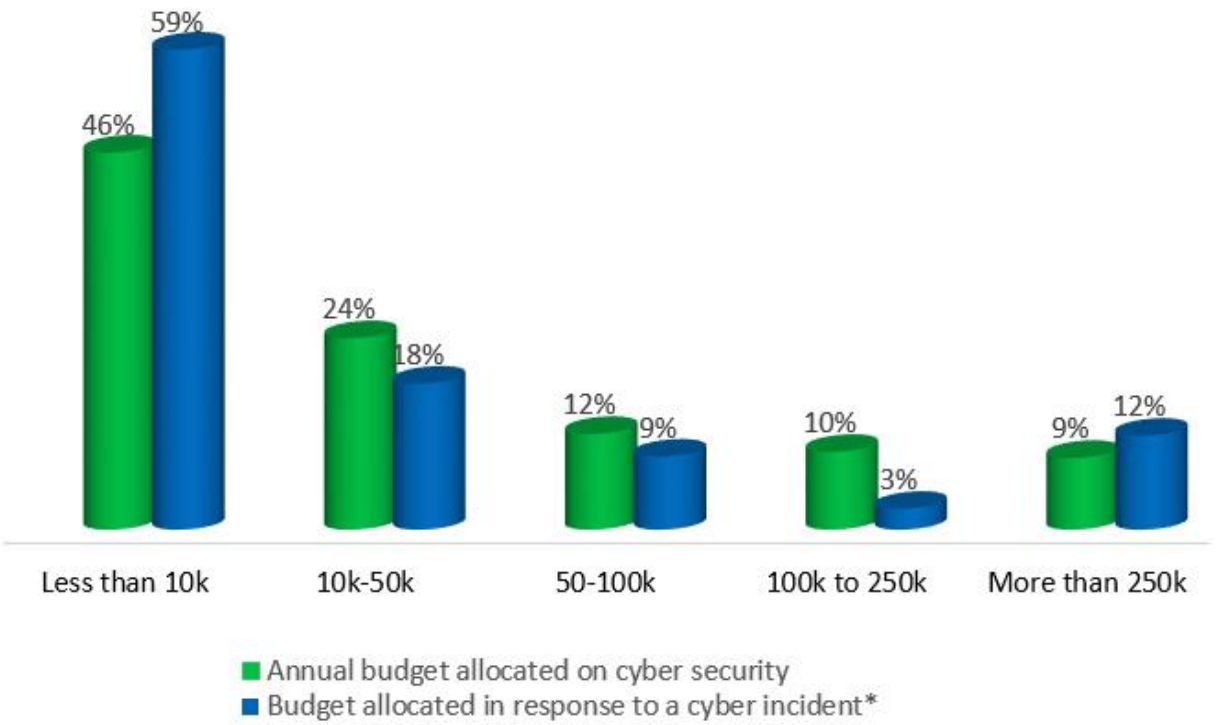
Knowledge about guidelines/cyber security take-up



Business continuity and validation

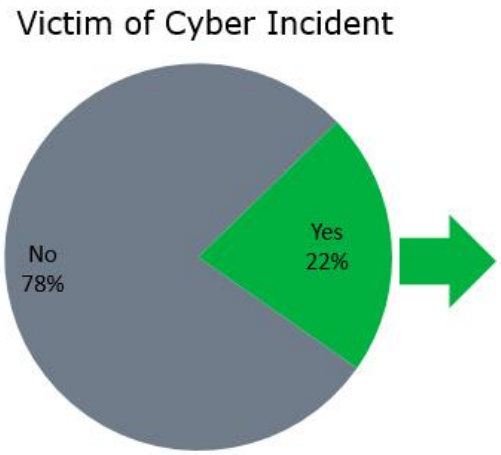


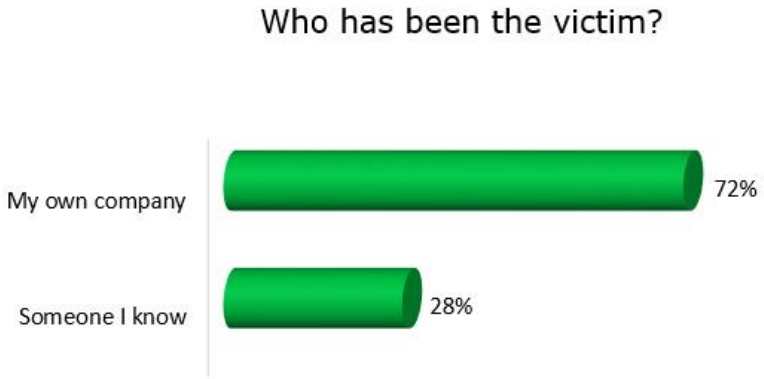
Budget allocation on cyber security



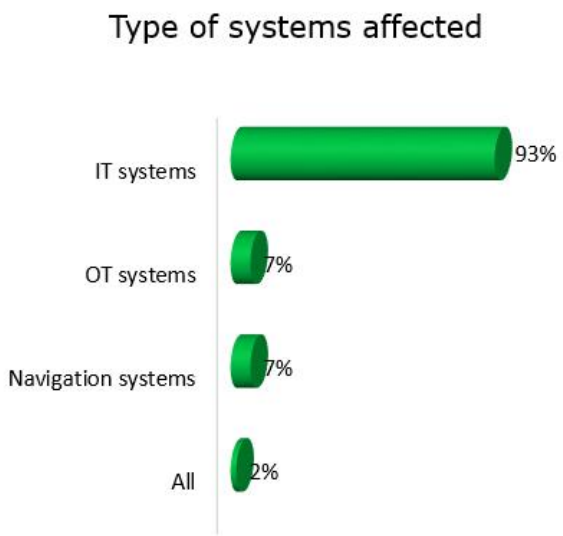
Incident insights from survey respondents

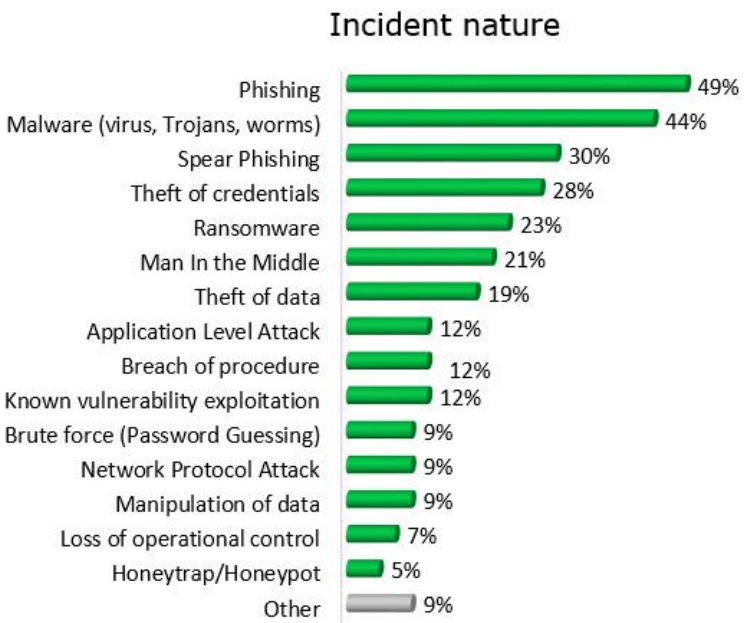
Incident specifics





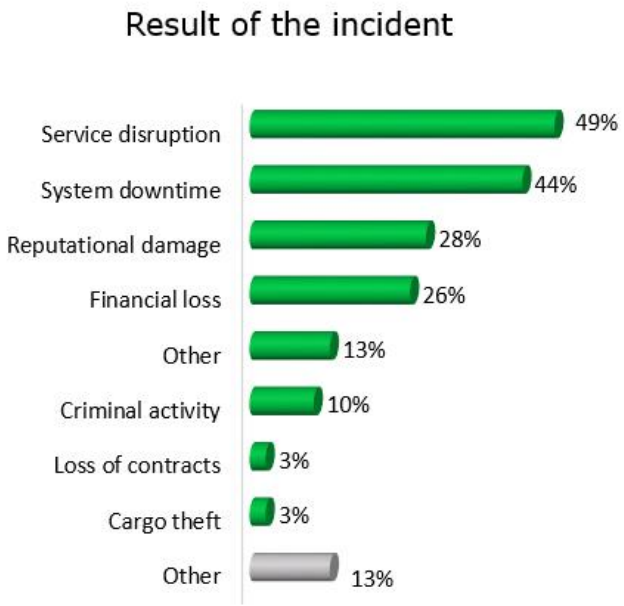
Systems and nature of incident



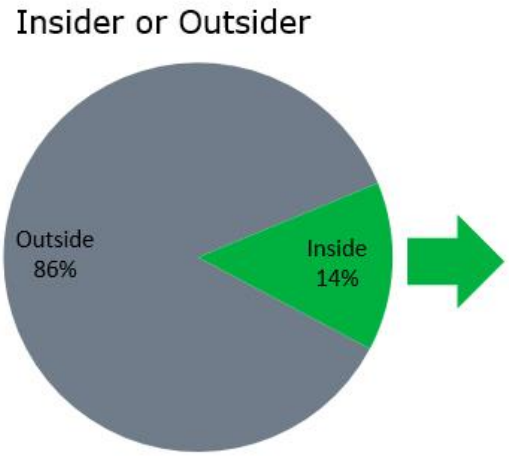


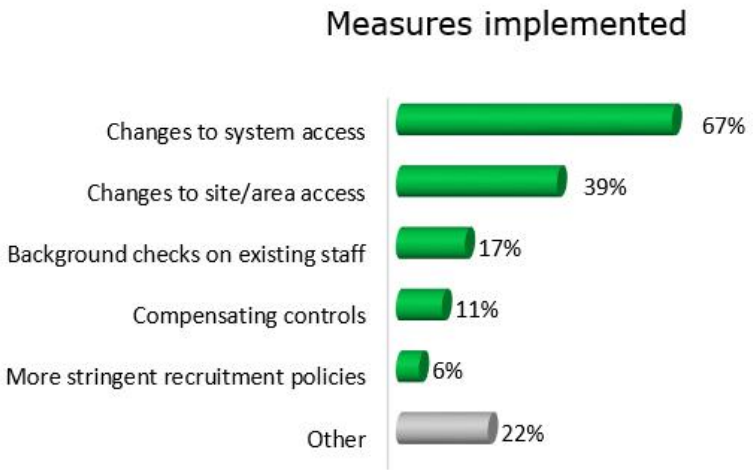
Detection time / extent of incident

Result and cost of incidents to business

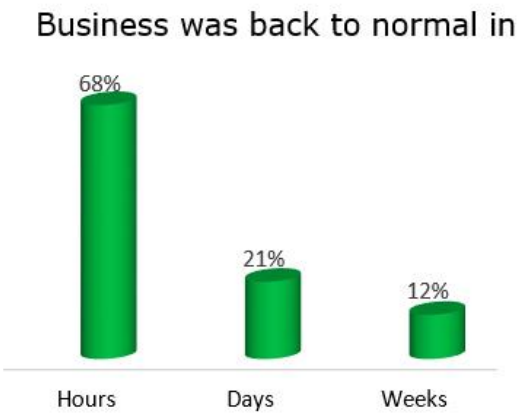


Origin of the attack

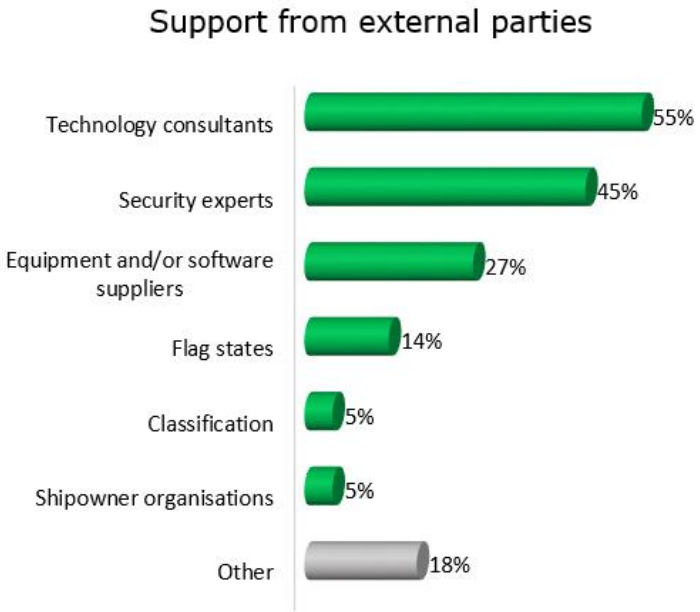




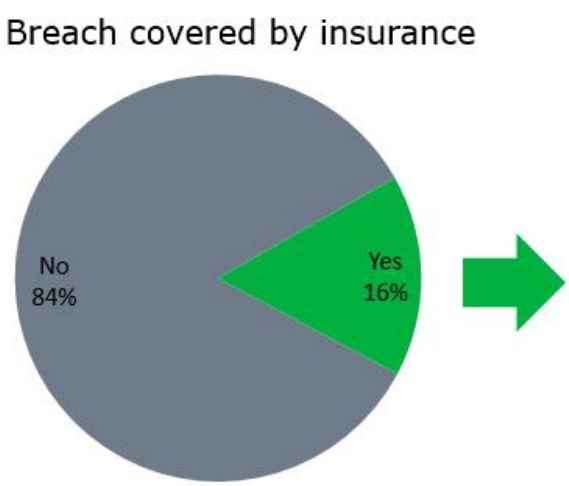
Getting things back to normal



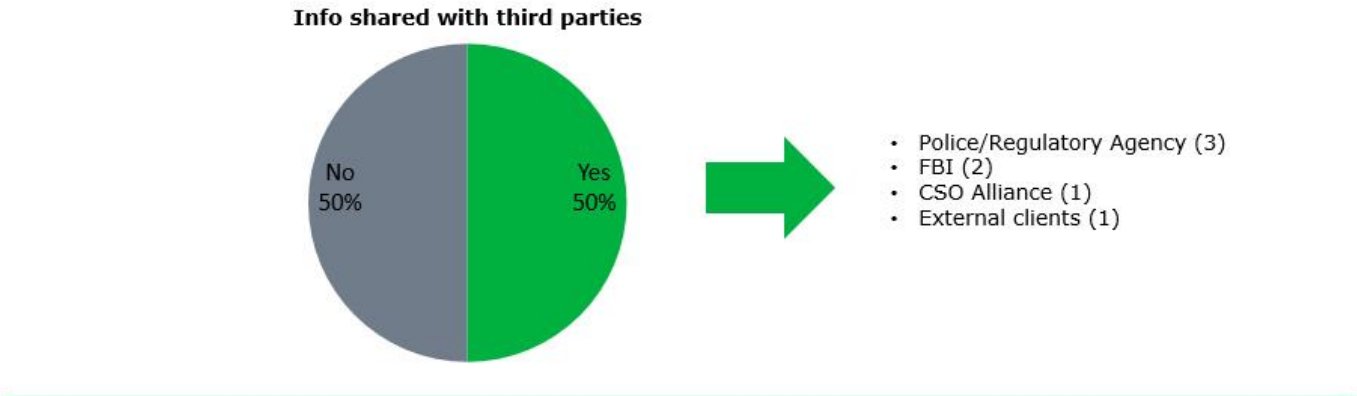
Incident knowledge and support from external parties

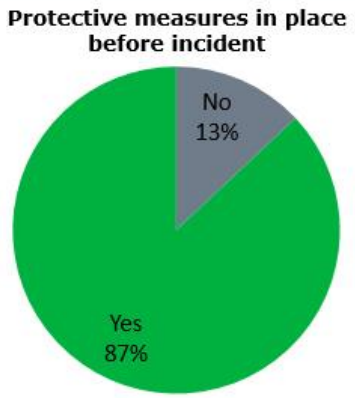


Cyber incident insurance coverage



Sharing of information and protective measures





How the results compare with previous years

Three key takeaways

- Attacks within last 12 months fell to 22% in 2018 for those answering “yes” from 34% in 2017 (21% in 2016); and increased to 78% for those answering “no” from 49% in 2017 (57% in 2016).
- “Theft of credentials” increased significantly as a reason behind cyberattack in 2018 to 28% of respondents, from just 2% in 2017. Phishing and Malware remained the top two reasons (49% and 44% in 2018).
- Crew training on rise: Those answering “no” to whether they had received training in cyber awareness decreased from 76% of crews responding in 2017 to 27% in 2018.

IHS Markit Customer Care:

CustomerCare@ihsmarkit.com
Americas: +1 800 IHS CARE (+1 800 447 2273)
Europe, Middle East, and Africa: +44 (0) 1344 328 300
Asia and the Pacific Rim: +604 291 3600

IHS Markit™