

Maritime Cyber Survey 2018 - the results

Not for onward distribution
Embargoed until 14/09/18

Fairplay

BIMCO



ABS

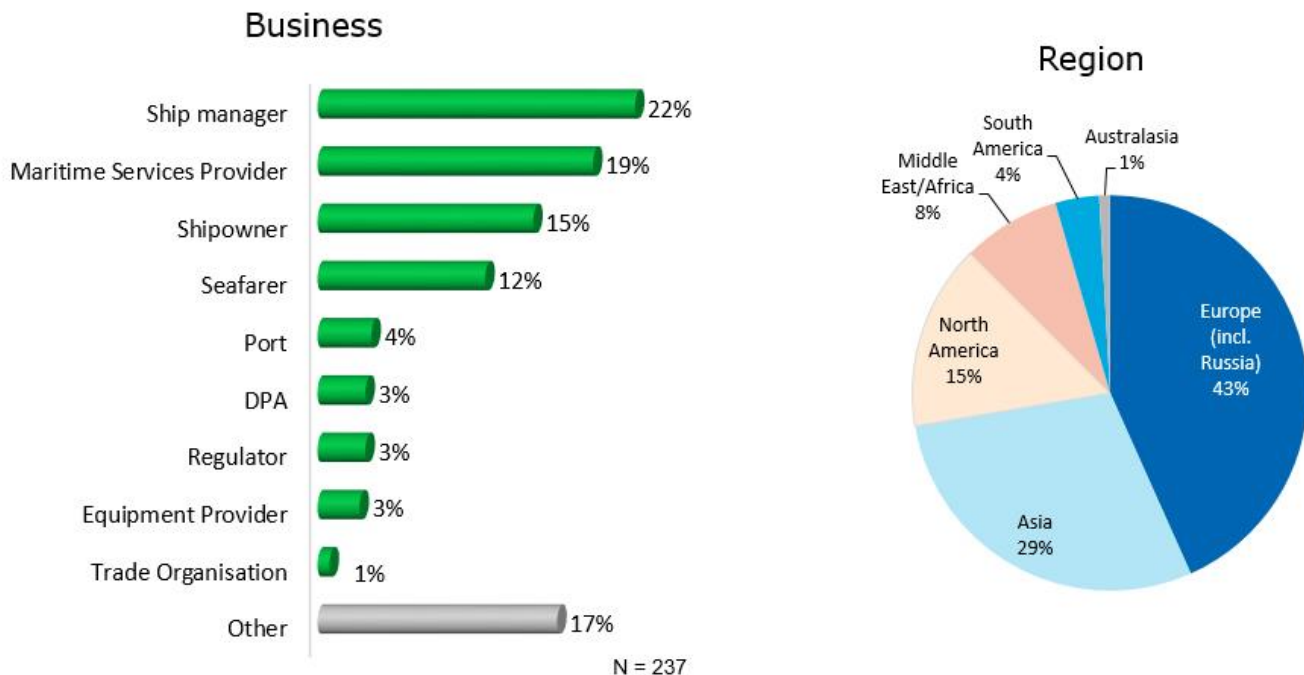
Advanced
Solutions

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.

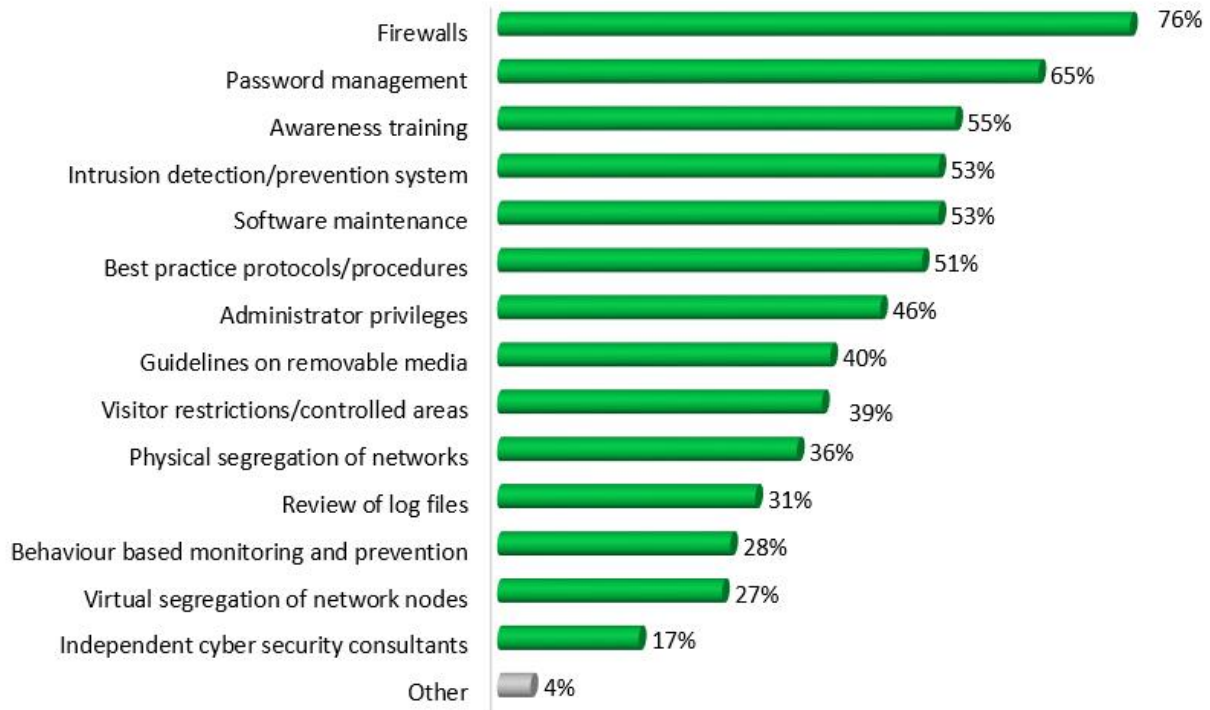
Who responded

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

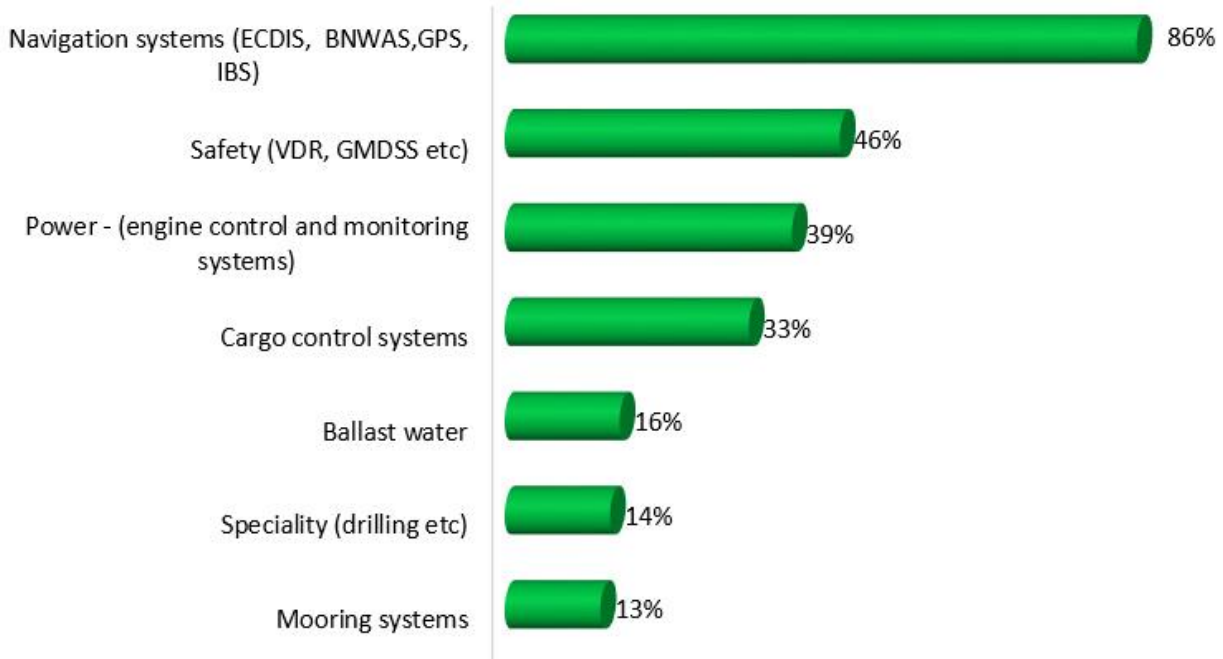


Industry overview: maritime's response to the cyber threat

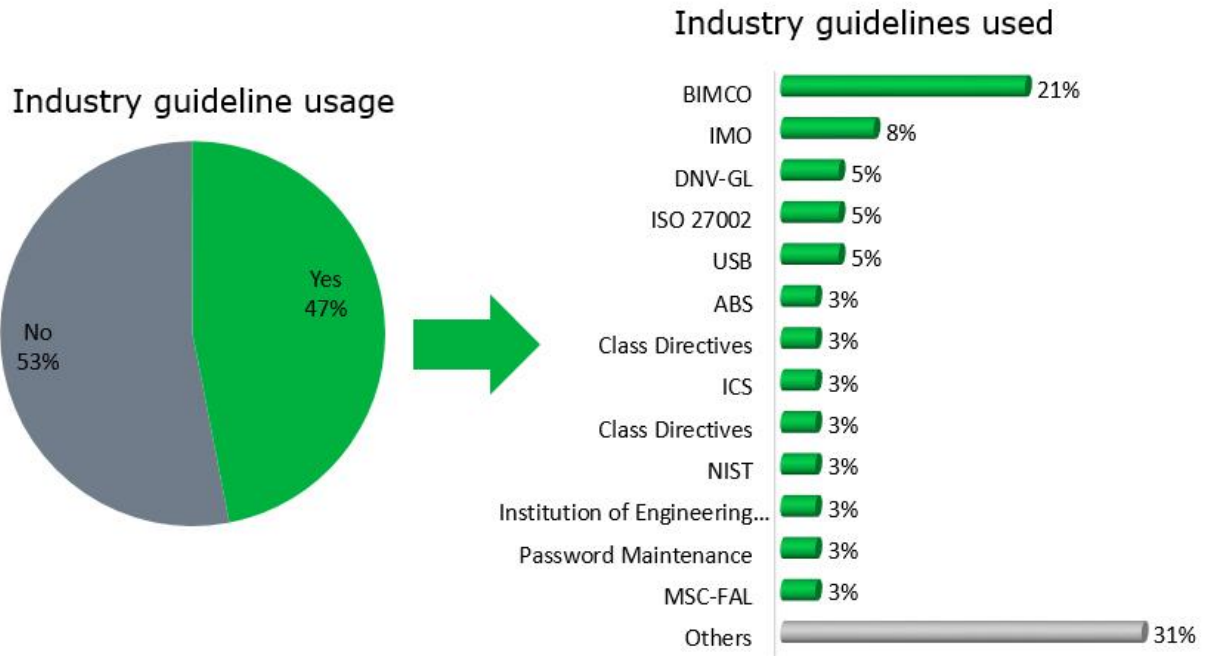
Measures being used for protection



Areas perceived as most vulnerable to attack

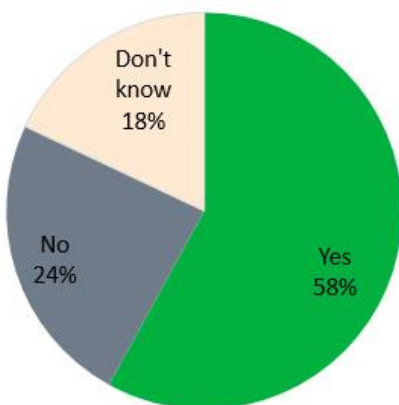


Take up of industry guidelines

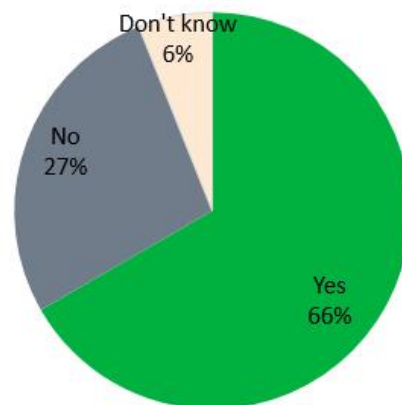


Knowledge about guidelines/cyber security take-up

Guideline incorporated

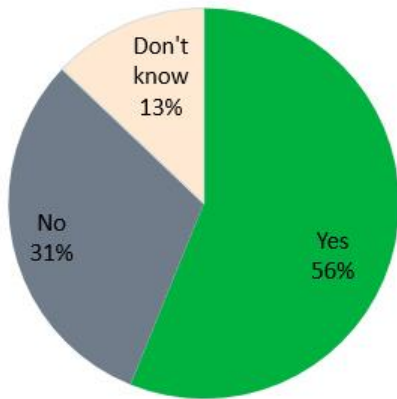


Undergone cyber security training

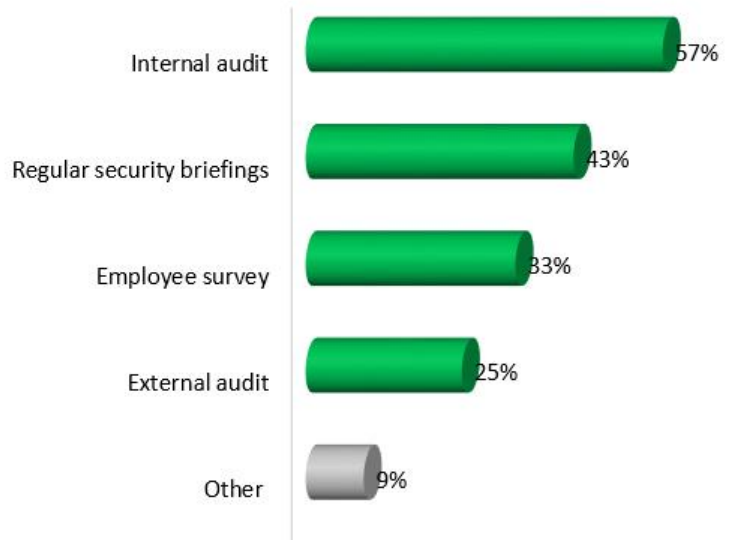


Business continuity and validation

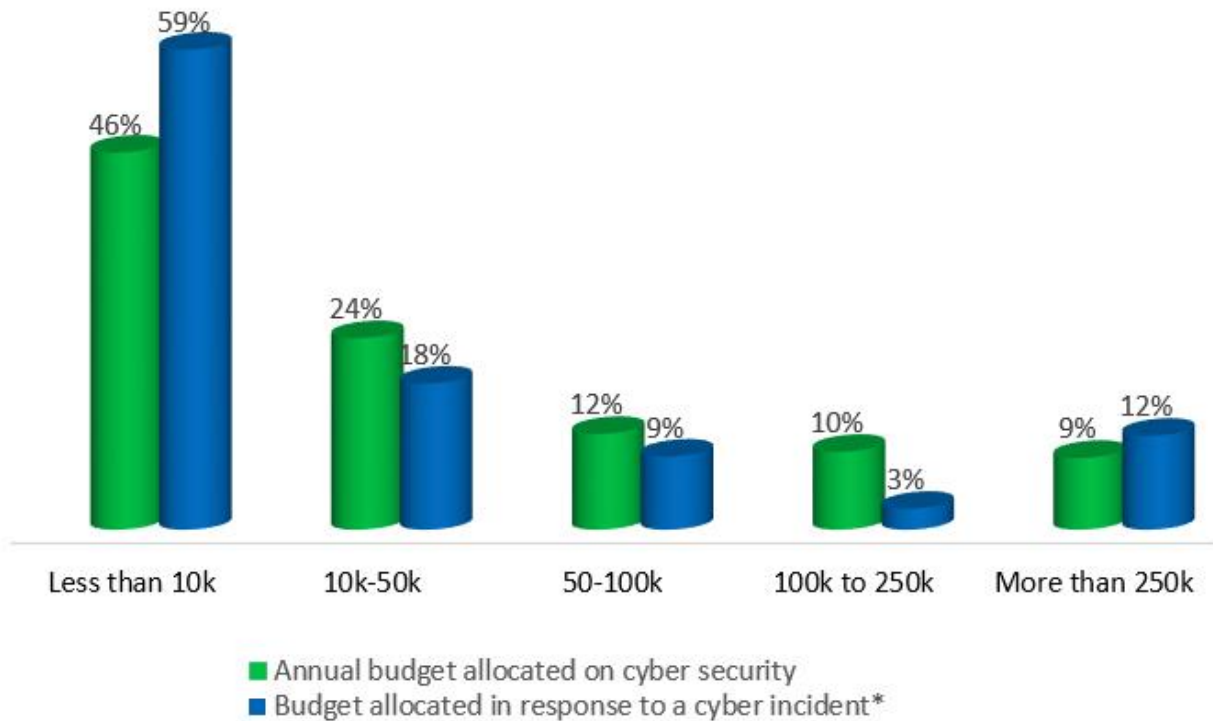
Business continuity plan



Cyber security validation



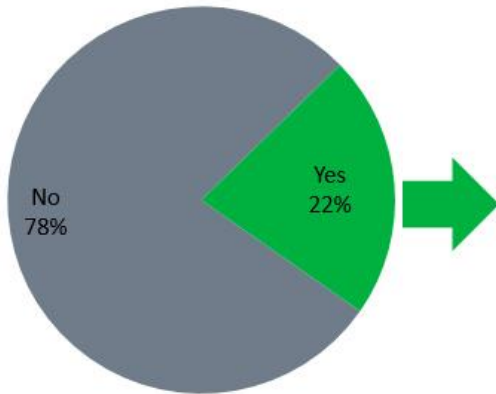
Budget allocation on cyber security



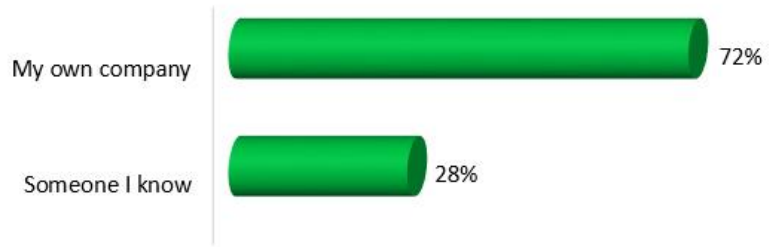
Incident insights from survey respondents

Incident specifics

Victim of Cyber Incident

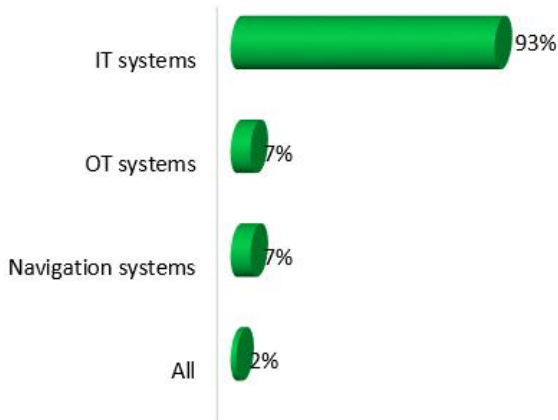


Who has been the victim?

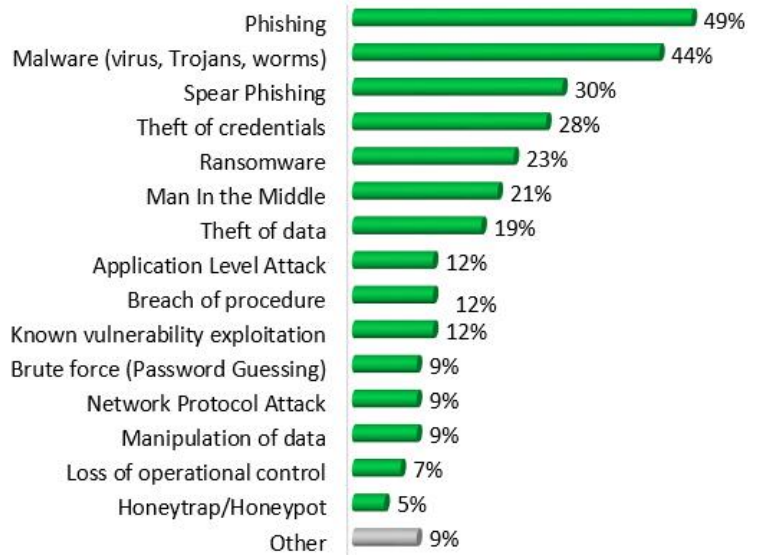


Systems and nature of incident

Type of systems affected



Incident nature

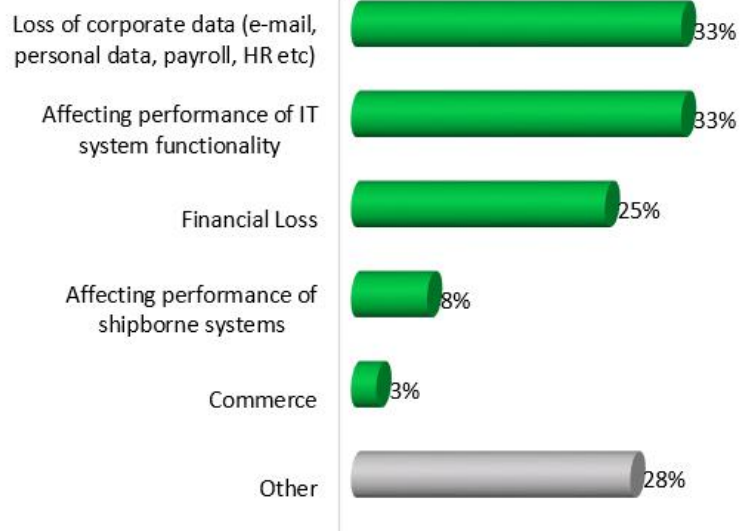


Detection time / extent of incident

Incident detection time

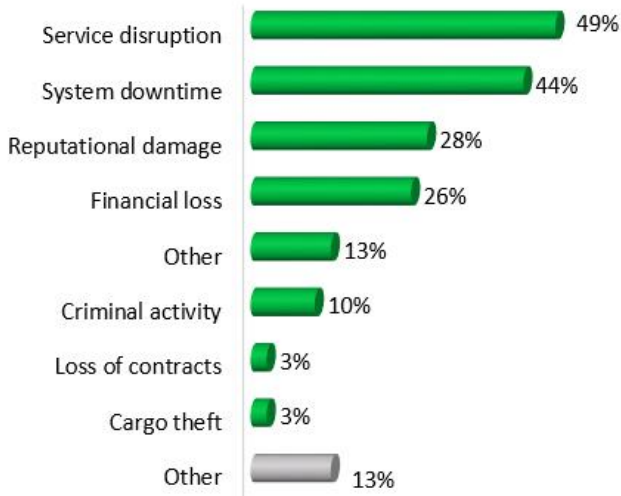


Incident extent



Result and cost of incidents to business

Result of the incident

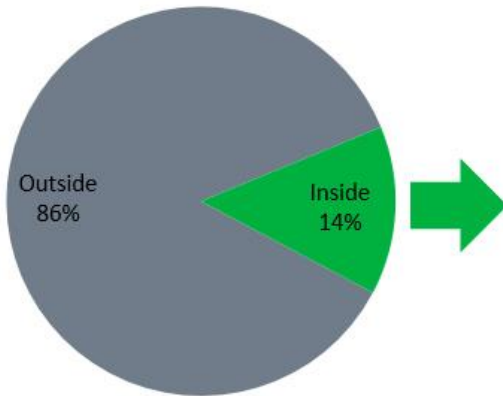


Cost of the incident

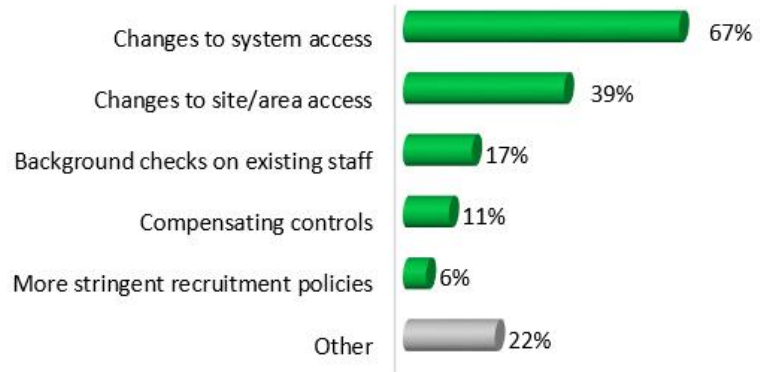


Origin of the attack

Insider or Outsider



Measures implemented

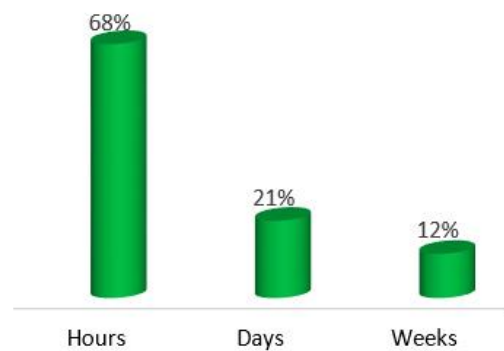


Getting things back to normal

Response & Recovery



Business was back to normal in



Incident knowledge and support from external parties

Knowledge of the incident

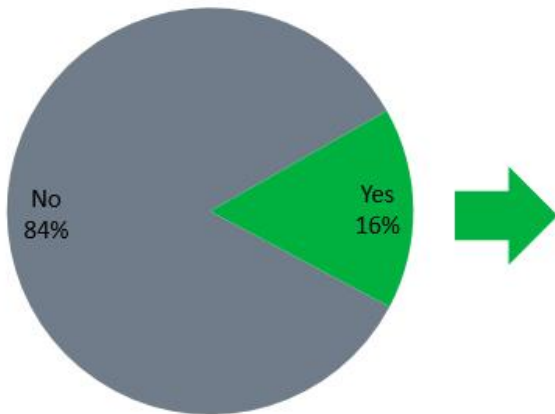


Support from external parties

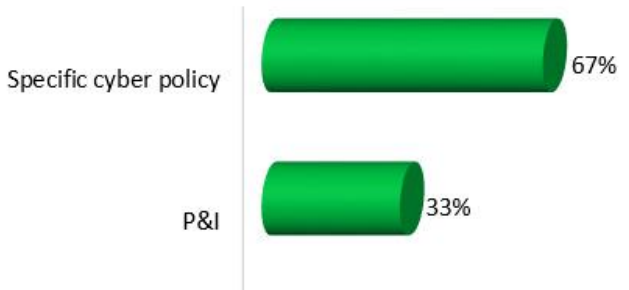


Cyber incident insurance coverage

Breach covered by insurance

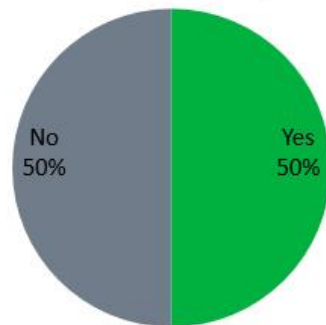


Policy used to claim



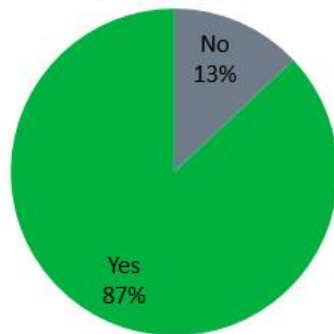
Sharing of information and protective measures

Info shared with third parties



- Police/Regulatory Agency (3)
- FBI (2)
- CSO Alliance (1)
- External clients (1)

Protective measures in place before incident



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

Disclaimer

The information contained in this report is confidential. Any unauthorized use, disclosure, reproduction, or dissemination, in full or in part, in any media or by any means, without the prior written permission of IHS Markit Ltd. or any of its affiliates ("IHS Markit") is strictly prohibited. IHS Markit owns all IHS Markit logos and trade names contained in this report that are subject to license. Opinions, statements, estimates, and projections in this report (including other media) are solely those of the individual author(s) at the time of writing and do not necessarily reflect the opinions of IHS Markit. Neither IHS Markit nor the author(s) has any obligation to update this report in the event that any content, opinion, statement, estimate, or projection (collectively, "information") changes or subsequently becomes inaccurate. IHS Markit makes no warranty, expressed or implied, as to the accuracy, completeness, or timeliness of any information in this report, and shall not in any way be liable to any recipient for any inaccuracies or omissions. Without limiting the foregoing, IHS Markit shall have no liability whatsoever to any recipient, whether in contract, in tort (including negligence), under warranty, under statute or otherwise, in respect of any loss or damage suffered by any recipient as a result of or in connection with any information provided, or any course of action determined, by it or any third party, whether or not based on any information provided. The inclusion of a link to an external website by IHS Markit should not be understood to be an endorsement of that website or the site's owners (or their products/services). IHS Markit is not responsible for either the content or output of external websites. Copyright © 2018, IHS Markit™. All rights reserved and all intellectual property rights are retained by IHS Markit.

