Maritime Cyber Survey 2018 - the results

Not for onward distribution
Embargoed until 14/09/18
### 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.

**Business**

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship manager</td>
<td>22%</td>
</tr>
<tr>
<td>Maritime Services Provider</td>
<td>19%</td>
</tr>
<tr>
<td>Shipowner</td>
<td>15%</td>
</tr>
<tr>
<td>Seafarer</td>
<td>12%</td>
</tr>
<tr>
<td>Port</td>
<td>4%</td>
</tr>
<tr>
<td>DPA</td>
<td>3%</td>
</tr>
<tr>
<td>Regulator</td>
<td>3%</td>
</tr>
<tr>
<td>Equipment Provider</td>
<td>3%</td>
</tr>
<tr>
<td>Trade Organisation</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>17%</td>
</tr>
</tbody>
</table>

**Region**

- Europe (incl. Russia): 43%
- Asia: 29%
- North America: 15%
- Middle East/Africa: 8%
- South America: 4%
- Australasia: 1%

N = 237
Industry overview: maritime’s response to the cyber threat

Measures being used for protection

- Firewalls: 76%
- Password management: 65%
- Awareness training: 55%
- Intrusion detection/prevention system: 53%
- Software maintenance: 53%
- Best practice protocols/procedures: 51%
- Administrator privileges: 45%
- Guidelines on removable media: 40%
- Visitor restrictions/controlled areas: 39%
- Physical segregation of networks: 36%
- Review of log files: 31%
- Behaviour based monitoring and prevention: 28%
- Virtual segregation of network nodes: 27%
- Independent cyber security consultants: 17%
- Other: 4%

Areas perceived as most vulnerable to attack

- Navigation systems (ECDIS, BNWAS, GPS, IBS): 86%
- Safety (VDR, GMDSS etc): 46%
- Power - (engine control and monitoring systems): 39%
- Cargo control systems: 33%
- Ballast water: 16%
- Speciality (drilling etc): 14%
- Mooring systems: 13%
Take up of industry guidelines

Industry guideline usage

Industry guidelines used

Knowledge about guidelines/cyber security take-up

Guideline incorporated

Undergone cyber security training
Business continuity and validation

**Business continuity plan**

- Yes: 56%
- No: 31%
- Don’t know: 13%

**Cyber security validation**

- Internal audit: 57%
- Regular security briefings: 43%
- Employee survey: 33%
- External audit: 25%
- Other: 9%

Budget allocation on cyber security

<table>
<thead>
<tr>
<th>Category</th>
<th>Less than 10k</th>
<th>10k-50k</th>
<th>50-100k</th>
<th>100k to 250k</th>
<th>More than 250k</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual budget</td>
<td>46%</td>
<td>24%</td>
<td>12%</td>
<td>10%</td>
<td>9%</td>
</tr>
<tr>
<td>Budget allocated</td>
<td>59%</td>
<td>18%</td>
<td>12%</td>
<td>3%</td>
<td>9%</td>
</tr>
</tbody>
</table>

*Green bar: Annual budget allocated on cyber security
*Blue bar: Budget allocated in response to a cyber incident*
 Incident insights from survey respondents

Incident specifics

Victim of Cyber Incident

No 78%
Yes 22%

Who has been the victim?

My own company 72%
Someone I know 28%

Systems and nature of incident

Type of systems affected

IT systems 93%
OT systems 7%
Navigation systems 7%
All 2%

Incident nature

Phishing 49%
Malware (virus, Trojans, worms) 44%
Spear Phishing 30%
Theft of credentials 28%
Ransomware 23%
Man in the Middle 21%
Theft of data 19%
Application Level Attack 12%
Breach of procedure 12%
Known vulnerability exploitation 12%
Brute force (Password Guessing) 9%
Network Protocol Attack 9%
Manipulation of data 9%
Loss of operational control 7%
Honeytrap/Honeypot 5%
Other 9%
Detection time / extent of incident

<table>
<thead>
<tr>
<th>Incident detection time</th>
<th>Incident extent</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-24 Hours</td>
<td>Loss of corporate data (e-mail, personal data, payroll, HR etc) 33%</td>
</tr>
<tr>
<td>0-6 Hours</td>
<td>Affecting performance of IT system functionality 33%</td>
</tr>
<tr>
<td>Immediately</td>
<td>Financial Loss 25%</td>
</tr>
<tr>
<td>Days</td>
<td>Affecting performance of shipborne systems 8%</td>
</tr>
<tr>
<td>Weeks</td>
<td>Commerce 3%</td>
</tr>
<tr>
<td>Months</td>
<td>Other 28%</td>
</tr>
</tbody>
</table>

Result and cost of incidents to business

<table>
<thead>
<tr>
<th>Result of the incident</th>
<th>Cost of the incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service disruption</td>
<td>Less than $5,000</td>
</tr>
<tr>
<td>System downtime</td>
<td>Between $5,000 and $50,000</td>
</tr>
<tr>
<td>Reputational damage</td>
<td>Between $100,000 and $500,000</td>
</tr>
<tr>
<td>Financial loss</td>
<td>Between $500,000 - $1 million</td>
</tr>
<tr>
<td>Other</td>
<td>Between $1 million and $10 million</td>
</tr>
<tr>
<td>Criminal activity</td>
<td>Between $50,000 and $100,000</td>
</tr>
<tr>
<td>Loss of contracts</td>
<td></td>
</tr>
<tr>
<td>Cargo theft</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>
Origin of the attack

- Inside: 14%
- Outside: 86%

Measures implemented:
- Changes to system access: 67%
- Changes to site/area access: 39%
- Background checks on existing staff: 17%
- Compensating controls: 11%
- More stringent recruitment policies: 6%
- Other: 22%

Getting things back to normal

Response & Recovery:
- Internal IT team: 76%
- Senior management team: 68%
- External IT consultants: 24%
- Suppliers: 21%
- Operational technology: 18%
- Whole company: 12%
- Ship's master/senior officers: 12%
- Insurers: 3%
- Ship's crew: 3%

Business was back to normal in:
- Hours: 68%
- Days: 21%
- Weeks: 12%
Incident knowledge and support from external parties

Knowledge of the incident
- Whole company: 61%
- Senior management team: 55%
- Internal IT team: 55%
- Top executive: 48%
- External IT consultants: 19%
- Ship's master/senior officers: 19%
- Insurers: 10%
- Ship's crew: 10%
- Public: 6%

Support from external parties
- Technology consultants: 55%
- Security experts: 45%
- Equipment and/or software suppliers: 27%
- Flag states: 14%
- Classification: 5%
- Shipowner organisations: 5%
- Other: 18%

Cyber incident insurance coverage

Breach covered by insurance
- No: 84%
- Yes: 16%

Policy used to claim
- Specific cyber policy: 67%
- P&I: 33%
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.