U.S. Maritime Industry Not Prepared for Future Cyber Attacks

Jones Walker LLP Releases Inaugural Maritime Cybersecurity Survey

Oct 24, 2018, 10:00 ET

NEWS PROVIDED BY
Jones Walker LLP

Jones Walker LLP Releases Inaugural Maritime Cybersecurity Survey

The U.S. maritime industry has a lot to lose — in fact, a whole lot to lose — and it's not ready for the next big cyber attack. A new survey by Jones Walker LLP, a multinational law firm, has found that nearly 70% of respondents believe the maritime industry is not prepared to handle the far-reaching business, financial, regulatory, and public relations consequences of a data breach.

The survey, conducted by Jones Walker's Information Security Practice and the Maritime Cybersecurity Survey, reflects the responses of 126 senior executives, chief information and technology officers, non-executive directors, and other maritime industry stakeholders. The respondents represent key sectors in the maritime industry and include professionals from small, mid-size, and large companies.

The survey shows that maritime companies are not prepared to handle a cybersecurity attack and that the industry is unprepared to shoulder the financial consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

The survey also found that maritime companies are not prepared to handle the business, financial, regulatory, and public relations consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

According to the survey, 48% of small company (1 to 49 employees) respondents and 19% of mid-size company (50 to 400 employees) respondents indicated preparedness. For many companies, insurance alone may not be enough to ensure preparedness.

“Several key findings of the Jones Walker Maritime Cybersecurity Survey demonstrate that every maritime industry stakeholder needs to take heed of the growing cybersecurity threats against our global maritime industry,” said Joel R. Whitehead, Director of Information Technology, Port Fourchon, Louisiana. “The survey strongly illustrates that industry preparedness is dependent on two factors: company size and recent experience as a cyber attack target.”

Whitehead noted that maritime companies face unprecedented cybersecurity threats and that the growing threat of cyber attacks is putting the maritime industry at risk. “The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.”

Jones Walker's Maritime Cybersecurity Survey demonstrates that every maritime industry stakeholder needs to take heed of the growing cybersecurity threats against our global maritime industry. The survey strongly illustrates that industry preparedness is dependent on two factors: company size and recent experience as a cyber attack target.

About Jones Walker

Jones Walker is a multinational law firm with more than 220 lawyers and government relations professionals in 21 offices across the United States and the Caribbean. Jones Walker has been named one of the Best Law Firms in the nation for 14 consecutive years by U.S. News & World Report and the Law Firm of the Year for multiple practice areas.

The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.

The U.S. maritime industry has a lot to lose — in fact, a whole lot to lose — and it's not ready for the next big cyber attack. A new survey by Jones Walker LLP, a multinational law firm, has found that nearly 70% of respondents believe the maritime industry is not prepared to handle the far-reaching business, financial, regulatory, and public relations consequences of a data breach.

The survey, conducted by Jones Walker's Information Security Practice and the Maritime Cybersecurity Survey, reflects the responses of 126 senior executives, chief information and technology officers, non-executive directors, and other maritime industry stakeholders. The respondents represent key sectors in the maritime industry and include professionals from small, mid-size, and large companies.

The survey shows that maritime companies are not prepared to handle a cybersecurity attack and that the industry is unprepared to shoulder the financial consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

The survey also found that maritime companies are not prepared to handle the business, financial, regulatory, and public relations consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

According to the survey, 48% of small company (1 to 49 employees) respondents and 19% of mid-size company (50 to 400 employees) respondents indicated preparedness. For many companies, insurance alone may not be enough to ensure preparedness.

“Several key findings of the Jones Walker Maritime Cybersecurity Survey demonstrate that every maritime industry stakeholder needs to take heed of the growing cybersecurity threats against our global maritime industry,” said Joel R. Whitehead, Director of Information Technology, Port Fourchon, Louisiana. “The survey strongly illustrates that industry preparedness is dependent on two factors: company size and recent experience as a cyber attack target.”

Whitehead noted that maritime companies face unprecedented cybersecurity threats and that the growing threat of cyber attacks is putting the maritime industry at risk. “The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.”

Jones Walker is a multinational law firm with more than 220 lawyers and government relations professionals in 21 offices across the United States and the Caribbean. Jones Walker has been named one of the Best Law Firms in the nation for 14 consecutive years by U.S. News & World Report and the Law Firm of the Year for multiple practice areas.

The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.

The U.S. maritime industry has a lot to lose — in fact, a whole lot to lose — and it's not ready for the next big cyber attack. A new survey by Jones Walker LLP, a multinational law firm, has found that nearly 70% of respondents believe the maritime industry is not prepared to handle the far-reaching business, financial, regulatory, and public relations consequences of a data breach.

The survey, conducted by Jones Walker's Information Security Practice and the Maritime Cybersecurity Survey, reflects the responses of 126 senior executives, chief information and technology officers, non-executive directors, and other maritime industry stakeholders. The respondents represent key sectors in the maritime industry and include professionals from small, mid-size, and large companies.

The survey shows that maritime companies are not prepared to handle a cybersecurity attack and that the industry is unprepared to shoulder the financial consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

The survey also found that maritime companies are not prepared to handle the business, financial, regulatory, and public relations consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

According to the survey, 48% of small company (1 to 49 employees) respondents and 19% of mid-size company (50 to 400 employees) respondents indicated preparedness. For many companies, insurance alone may not be enough to ensure preparedness.

“Several key findings of the Jones Walker Maritime Cybersecurity Survey demonstrate that every maritime industry stakeholder needs to take heed of the growing cybersecurity threats against our global maritime industry,” said Joel R. Whitehead, Director of Information Technology, Port Fourchon, Louisiana. “The survey strongly illustrates that industry preparedness is dependent on two factors: company size and recent experience as a cyber attack target.”

Whitehead noted that maritime companies face unprecedented cybersecurity threats and that the growing threat of cyber attacks is putting the maritime industry at risk. “The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.”

Jones Walker is a multinational law firm with more than 220 lawyers and government relations professionals in 21 offices across the United States and the Caribbean. Jones Walker has been named one of the Best Law Firms in the nation for 14 consecutive years by U.S. News & World Report and the Law Firm of the Year for multiple practice areas.

The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.

The U.S. maritime industry has a lot to lose — in fact, a whole lot to lose — and it's not ready for the next big cyber attack. A new survey by Jones Walker LLP, a multinational law firm, has found that nearly 70% of respondents believe the maritime industry is not prepared to handle the far-reaching business, financial, regulatory, and public relations consequences of a data breach.

The survey, conducted by Jones Walker's Information Security Practice and the Maritime Cybersecurity Survey, reflects the responses of 126 senior executives, chief information and technology officers, non-executive directors, and other maritime industry stakeholders. The respondents represent key sectors in the maritime industry and include professionals from small, mid-size, and large companies.

The survey shows that maritime companies are not prepared to handle a cybersecurity attack and that the industry is unprepared to shoulder the financial consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

The survey also found that maritime companies are not prepared to handle the business, financial, regulatory, and public relations consequences of a data breach. In contrast, 97% of large company respondents have cyber insurance coverage.

According to the survey, 48% of small company (1 to 49 employees) respondents and 19% of mid-size company (50 to 400 employees) respondents indicated preparedness. For many companies, insurance alone may not be enough to ensure preparedness.

“Several key findings of the Jones Walker Maritime Cybersecurity Survey demonstrate that every maritime industry stakeholder needs to take heed of the growing cybersecurity threats against our global maritime industry,” said Joel R. Whitehead, Director of Information Technology, Port Fourchon, Louisiana. “The survey strongly illustrates that industry preparedness is dependent on two factors: company size and recent experience as a cyber attack target.”

Whitehead noted that maritime companies face unprecedented cybersecurity threats and that the growing threat of cyber attacks is putting the maritime industry at risk. “The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.”

Jones Walker is a multinational law firm with more than 220 lawyers and government relations professionals in 21 offices across the United States and the Caribbean. Jones Walker has been named one of the Best Law Firms in the nation for 14 consecutive years by U.S. News & World Report and the Law Firm of the Year for multiple practice areas.

The survey results, which were announced at the Marine Technology Society and IEEE Oceanic Engineering Society conference in New Orleans, reflect the need for urgent action by both industry and political leaders.