Insights Into the Changing Landscape of Cyber Insurance

**This article was originally published by Marine Log.*

Aug 29, 2023

Categories:

Publications
Technology Blog

Authors:

Gene F. Price

Pick your industry and you will quickly conclude that cyber-attacks on their systems are an empirical threat to commercial and industrial operations. Cyber risk now slices through almost every type of business activity, and the maritime industry is no exception. According to U.S. Coast Guard Cyber Command statistics, maritime cyber incidents increased 68% in 2021 alone.

Cyber-insecurity not only poses increased risks to maritime operations but also to general planning, which more and more has begun to rely on cyber insurance for predictable outcomes. According to BlackBerry, about 60% of businesses surveyed said they would actually reconsider making an agreement with a vendor if they learned that a vendor lacked comprehensive cyber-risk coverage.

Yet acquiring cyber insurance isn't as easy as it was a few years ago. Cyber premiums have soared as attacks have increased, with U.S. costs increasing over 50% from 2021 to 2022. AM Best reported that cybersecurity premiums collected reached $7.2 billion in 2022, indicating that losses from cybersecurity incidents have had a similar upward spiral.

Cyber Risks for Maritime Operations

Insurers are getting better at calculating their own risk when selling cyber policies and are trying to mature this type of insurance product. To this end, they are taking an ever-more critical look at applications for cyber insurance, and again, the maritime industry is not excluded. Shore-side maritime infrastructure, like ports and terminals, are much like other land-based activity from a cyber-attacker's point of view. A commercial building with internet access and email is common to almost every industry. But vessel networks can be quite different. While information technology (IT) systems for business and crew support similarly include email access, this

may be provided by pier-side connections to a foreign internet provider, introducing added risk.

Vessel networks are also not as readily "segmented" as shore-based enterprises. This can mean it is easier for a cyber-attacker to move laterally within a ship's IT network because user certification requirements are insufficient or nonexistent. It's also harder to receive critical software patches for security updates when a vessel is underway. The expense of using very small aperture terminal satellite systems can make it almost prohibitive to retrieve these updates, particularly when patches consist of large data files.

Adding to that, many ships have an operational technology (OT) network, which may regulate a vessel's industrial control systems, supervisory control and data acquisition (SCADA) systems, and other types of maritime OT networks. There should be a defined demilitarized zone or "DMZ" that blocks IT traffic from entering a vessel's OT network, but that is not always a certainty. A careless person with a flash drive, an unguarded internet access point in an OT network, or a remote connection can each be an attack vector for malware in an OT network, the effects of which can be extremely damaging. This could include compromising the navigation, vessel access, cargo handling, or communication systems.

Fortunately, spiraling cyber insurance costs appear to be dissipating. Cyber rates dropped around 10% in June 2023 compared to a year earlier, according to UK-based insurance broker Howden. Fitch Ratings is forecasting that U.S. cyber insurance premiums will likely stabilize this year. Barring some new development that again drives prices upward, it could be a good time to lock in coverage if you need cyber insurance or are up for a renewal.

Planning Considerations for Cyber Insurance

Having cyber insurance not only keeps a company covered; a policy's underwriting requirements should also improve a network's cybersecurity posture. As recognized by the Atlantic Council, cyber insurers play a crucial role in promoting effective cyber risk-management practices, which is often reflected in investments by

insureds in improved cyber defenses and training.

Cyber liability insurance features two main types: First-party insurance, which primarily covers an insured's losses from a cyber incident, and a somewhat more complex type, third-party cyber insurance. Third-party insurance covers an insured for third-party losses arising from a cyber incident. Regardless of the type of insurance a company wishes to acquire, it should begin by understanding its cybersecurity risks and insure over them appropriately.

In addition to expenses like system restoration, legal representation, and perhaps paying a ransom, consideration should be given to how the company would be impacted by a business shutdown due to a cyber-attack. It should also understand whether the company needs coverage for repair and restoral expenses only, or if coverage is needed to replace or recreate data and software irretrievably encrypted in a ransomware attack.

Understanding other types of insurance that may provide coverage is important, too, and will depend on the existing policies a company carries. For instance, some commercial general liability policies cover personal and advertising injury, which may include coverage when the publication of the organization's stolen data leads to privacy claims. Similarly, and again dependent upon a company's existing coverage, property or business interruption policies might cover data breaches that result in damage to enterprise systems.

Nevertheless, the prudent course of action is usually acquiring a dedicated cyber insurance policy that accounts for the costs of engaging an investigative forensic company, a law firm to manage the breach, and other associated expenses. Comprehensive policies are best, as they cover costs associated with all types of cyber-attacks, including penalties and fines arising from regulatory responses.

Once a company has undergone a thorough risk assessment to determine the kind of cyber insurance it needs, it should engage an insurance broker to help obtain cyber insurance and satisfy any requirements associated with the policy. For instance, some

insurers want insured companies to employ multi-factor authentication, have tested backups for each system or network, and use network segmentation to limit the ability of an attacker to infect a network. An informed broker should understand how to effectively deal with those issues. After acquiring the insurance, a broker can also be important in determining when and how notice should be provided to the insurer of possible claims.

Cyber insurance still isn't as inexpensive as it was just a few years ago, but with premium increases apparently abating, now may be a good time to purchase the best insurance for your company. By all accounts, cyber-attacks targeting the maritime and logistics industries are real and persistent threats, and unlike insurance premiums, there's little indication these attacks will diminish in the near future. The evidence points, unfortunately, to shoal waters ahead.

For more information, contact the author or any attorney with Frost Brown Todd's Data Security & Privacy team.

FBT Gibbons