Proactive Security Measures for Global Maritime Shipping

Shipping Companies Analysis In December 2021

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

111 West 33rd Street Floor 11
New York, NY 10001
1.800.682.1707

Background

The world's shipping nearly stopped last year when a huge tanker ran aground in the Suez canal, costing the shipping industry tens of millions of dollars every day until the ship was freed[1]. What would happen if there was a cyber attack on the shipping industry?

Global supply shortages and shipping disruptions brought on by the COVID-19 pandemic, pose a threat to our maritime security, and threaten to deprive families of a present-filled holiday celebrations. The maritime shipping network, which is responsible for 90% of the global trade[2], has gone from being a fast and cost-effective system to one plagued by delays, clogged shipping lanes[3], and exorbitant prices.

Already strained and taxed by the pandemic, a potential cyber incident in the shipping industry could have catastrophic effects on families, businesses, and workers all across the world.

Shipping Companies Analysis

In December 2021, SecurityScorecard conducted an analysis of the cybersecurity health of 100 global shipping container companies compared to the Forbes Global 2000[4] companies. The analysis reveals that high severity cyber vulnerabilities pose a significant risk to U.S. maritime security.

Key Findings

- Overall, the cybersecurity risk posture of the shipping industry was better than the Forbes Global 2000, but the shipping industry did not perform higher in every risk group factor.
- The largest risks to the sector include vulnerabilities in application security, irregular patching cadence, and network security.
- Data breach percentages for shipping container companies increased from 2018 through 2021, indicating that the industry may be an increasingly attractive target for malicious cyber actors during the 2021 winter holiday season.

[1] https://www.bbc.com/news/business-56559073.

[2] Sen. Gary Peters, Opening statement, Senate Commerce, Science, & Transportation Committee hearing, "Uncharted Waters: Challenges Posed by Ocean Shipping Supply Chains,"
Dec. 7, 2020,

[3] https://www.commerce.senate.gov/2021/12/uncharted-waters-challenges-posed-by-ocean-shipping-supply-chains.
Reuters, "Clogged shipping lanes threaten holiday sales," Oct. 7, 2021, https://finance.yahoo.com/video/clogged-shipping-ports-threaten-holiday-100454731.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJxewJKKSwL6m9f9sJcsMl9mZj5p7ig-9fPXdyL4K6SV8YVYbWE9N-_3-mQ5F_VcMAYWWP_fUEORxrde4qg7cB55zZ-W8RofgFACyTXF4ZR2hrRRrprZZXKP3ypKGimGQLBnKZgpFYAWbfBvRhQcGZqp37QzUm41AkC9V34Vc7k_.

[4] https://www.forbes.com/lists/global2000/#4a94c6f85ac0.

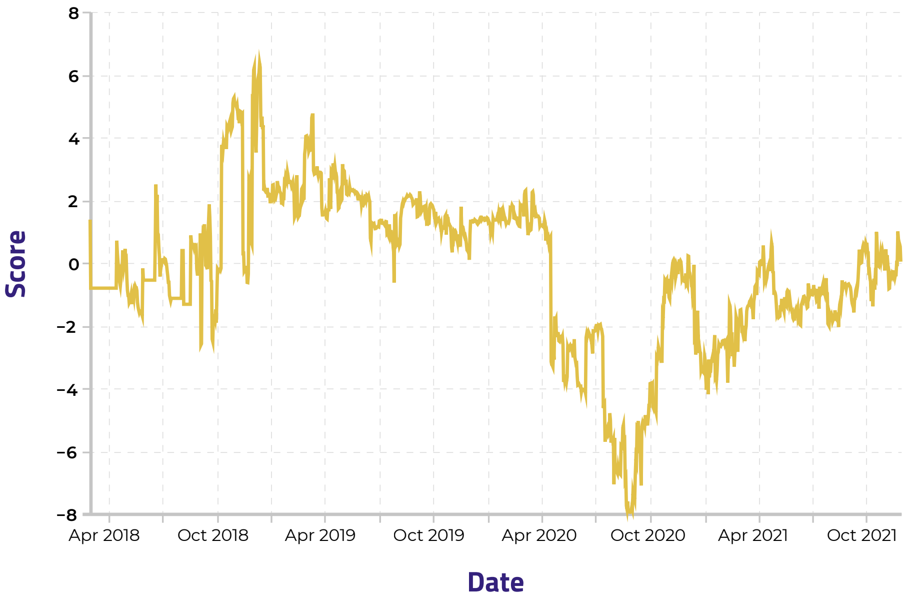
Measuring Cyber Risk On the High Seas

Overall Security Scores

Security leaders across the maritime industry should proactively increase their cybersecurity posture to defend against malicious cyber actors, but there is good news over the horizon.

Shipping container companies initially did better than the Forbes Global 2000 until April 2020, when high-profile attacks sank the industry average[5]. Since mid-2020, shipping container companies have continued to struggle to build resilience in their cybersecurity, and have not yet returned to their pre-2020 breach scores.

Median total scores difference (Container Shipping - Forbes 2000) **by day**



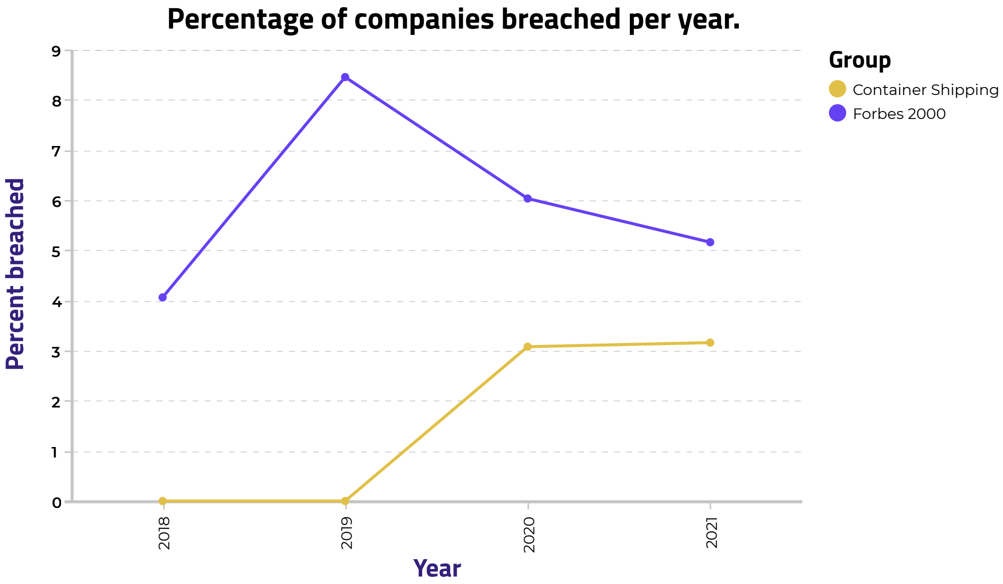
Annual Security Breaches

On a year-to-year basis, a lower percentage of global shipping domains were breached than the Forbes Global 2000. In 2018 and 2019, we observed virtually zero data breaches for shipping containers, which starkly contrasts with the Forbes Global 2000, where 4% of companies were breached in 2018 and 9% fell victim in 2019.

The Forbes Global 2000 list contains several hundred finance companies as well as companies that process other personal data. On the whole, shipping companies process

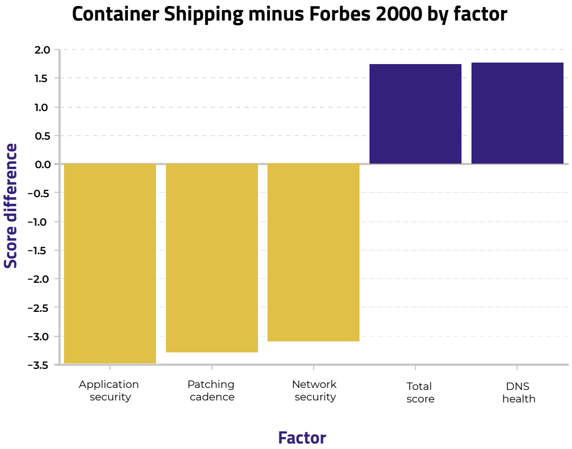
[5] To construct the comparative analysis SecurityScorecard calculated a median overall security score over time and the distribution of scores within each cohort.

less personal data. The attractiveness of personal data may account for the differences in data breaches.



A Deep Dive Into Risk Factors

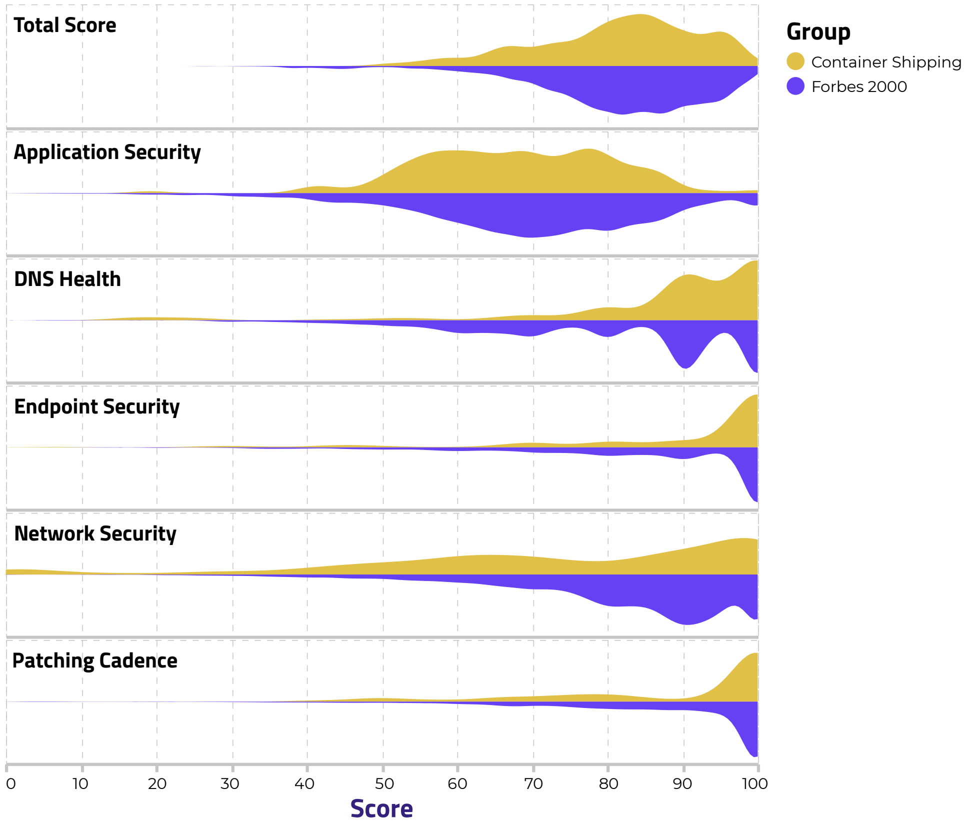
To probe the shipping industry in depth, we compared the median scores of shipping container companies with Forbes Global 2000 companies during the month of November 2021. Median scores between the two groups reveal specific concerns for the maritime industry.



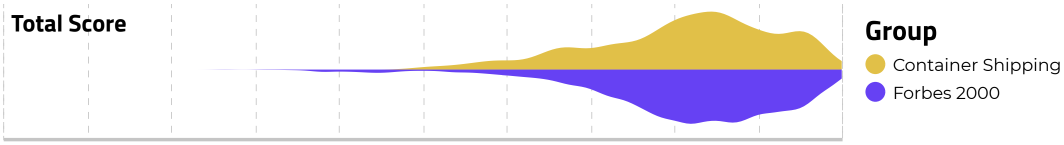
The risk group factors in purple show that shipping containers outperform the Forbes Global 2000. Risk factors in yellow show that Forbes Global 2000 companies are more secure than shipping container companies.

While shipping container companies show healthier DNS practices and a higher median total score, the industry exhibits alarming concerns for network security, patching cadence, and especially application security, which reveals a practically significant security rating of -3.5 points.

Mirror density plots for Container Shipping and Forbes 2000

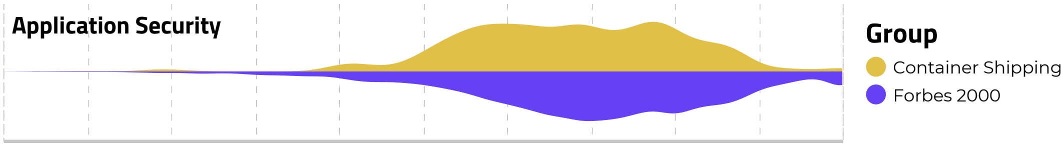


Even though the **mode score (total)** for both the shipping container companies and Forbes Global 2000 is a ‘B’, the shape of the distribution shows that shipping container companies tend to have better scores than Forbes Global 2000, with a larger variance

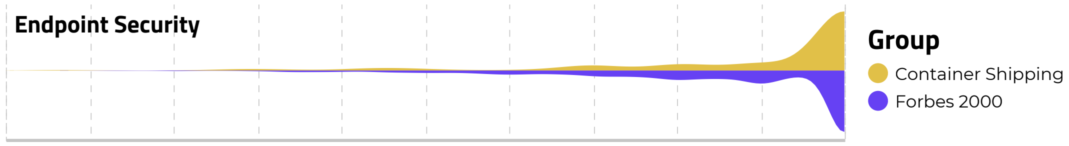


and a tail of companies with a score of ‘F.’

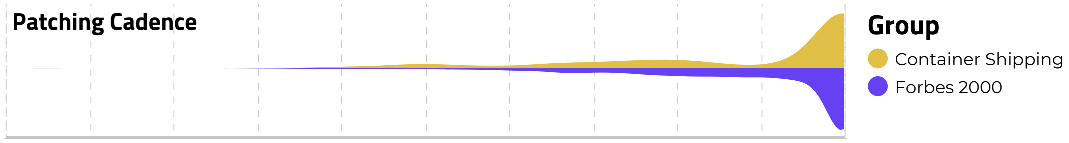
Analysis of **application security** revealed that both shipping containers and Forbes Global 2000 have mode scores in the ‘C’ letter grade range; shipping containers also have a noticeable set of companies who have a score between 60-70, favoring the Forbes Global 2000.



Analysis of **endpoint security**[6] revealed that both Forbes Global 2000 and shipping container companies have high numbers with perfect scores. However, there is a long tail of companies among both that have a letter grade of an ‘F,’ indicating significant variance among the sector. It also suggests the uneven security practices in each cohort do not comport with security best practices.



Although there are multiple companies in both cohorts with a perfect score for **patching cadence**, the mode score for Forbes Global 2000 is higher (in the high-80s), while shipping containers fall behind with a mode score of low 80s / high 70s. This is notable especially because there is an observable number of companies for Forbes Global 2000 who have a score below a 30–which lowers the overall mode of the cohort. Such a finding suggests the shipping industry, on average, might struggle with patching vulnerabilities at a regular interval. This observation could simply reflect the global, mobile, and diffuse nature of the industry as measured across the dynamic threat landscape in which all companies operate.

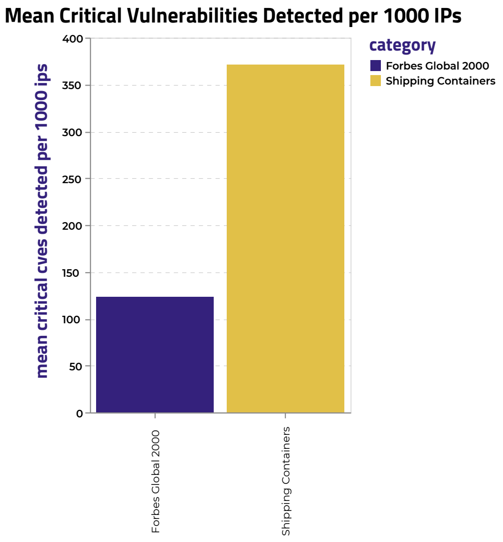


Patching cadence is about securing vulnerabilities.

The Common Vulnerabilities and Exposure (CVE) program (**https://www.cve.org/**) classifies vulnerabilities by severity, with critical being the most severe. We used this publicly available database of CVEs to measure the number of critical CVEs an entity has per 1,000 IP addresses to make a fair comparison.

An entity that has critical CVEs on all its IP addresses is exposed to greater cybersecurity

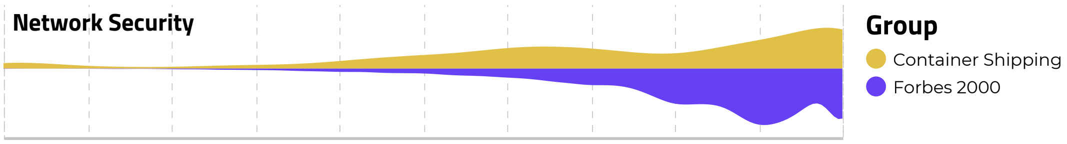
[6] The Endpoint Security module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins.



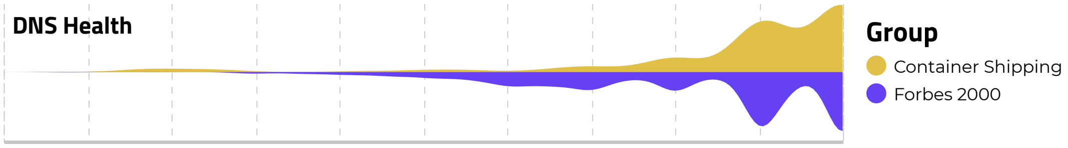
risks than an entity that has a critical CVE on a single IP address. The chart below shows critical CVEs for both groups, revealing that container shipping companies have far more vulnerabilities than the Forbes Global 2000.

The collective results of patching cadence and critical vulnerabilities suggest that global shipping companies must make patching their systems a priority in order to harden their security posture.

It also indicates that investors, or companies contracting with shipping containers, should ask hard questions about patching protocols and capabilities to ensure their sensitive data will be secure.



Analysis of **network security** revealed that both Forbes Global 2000 and shipping containers have a high number of companies with perfect scores. Each cohort includes a large group of companies with a letter grade of ‘A.’ There is a noticeable bubble of companies for shipping containers that have a score below a 10, which lowers the median network security score for shipping container companies below the Forbes Global 2000.



Analysis of **DNS Health** revealed both Forbes Global 2000 and shipping containers have a group of companies with a perfect score and have mode scores of a letter grade ‘A’. Forbes Global 2000 has a distinguishable number of companies with scores equivalent to a ‘D’ or an ‘F.’ Despite DNS favoring shipping container companies, both Forbes Global 2000 and shipping container companies have a tail of extremely low ‘F’ ratings.

Conclusion

A smooth sea never made a skilled sailor

No one knows when the world will recover from the COVID-19 pandemic, when shipping lanes will clear the holiday backlog, or when supply lines will unkink from these compounding challenges and thrive once again. What companies can do today is build resilience and develop risk mitigation strategies to defend against known cyber threats.

About SecurityScorecard

Funded by world-class investors including Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 + million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn.**

To receive an email with your company's current score, please visit
securityscorecard.com/instant-security-scorecard

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
111 West 33rd Street Floor 11
New York, NY 10001