Global Supply Chains under Increased Cyber Threats

Jan 06, 2023

Categories:

Publications
Technology Blog

Authors:

Brion St. Amour
Eric A. Baker
Tyler P. Biddle
Gene F. Price

With the arrival of 2023, we have some thoughts on the ever-growing cyber threats to our digital infrastructure. Foremost is the reality that supply chains are becoming favored targets. They share substantial amounts of data across multiple networks with enterprises whose abilities to withstand an attack are often unknown. They enjoyed increased revenues during COVID, with some companies sitting on large cash reserves. Nation-states recognized the crucial role logistics plays among interdependent economies. These and other factors attracted cyber-criminals and rogue nations looking for quick profits or disruption.

This attention comes at a shaky moment in the history of supply chains with no sector of the industry left unaffected; trucking, maritime, aviation, and multi-modal terminals have each seen preparations for attacks and incidents alike.

For instance, Expeditors, a Seattle logistics company, was hacked in February. The company shut down most of its IT network, saying it had "limited ability to conduct operations." Some suspect the hack was a ransomware attack.[1] The aviation industry was similarly targeted with attacks on major airports.[2] Microsoft announced that damaging ransomware attacks against transportation and logistics companies in Ukraine and Poland were linked to Russia.[3]

Russian digital reconnaissance was noted by Dragos in transportation infrastructure in the Netherlands. The actors they observed probing terminals in Rotterdam have ties to the GRU (Russian Military Intelligence) according to the FBI. The GRU was infamously blamed for the devastating "NotPetya" cyberattacks of 2017, which cost Danish shipper Maersk more than $300,000,000.[4] Hellmann Worldwide Logistics sustained a cyber-attack in December 2021 that disrupted operations for weeks. Trucking company Marten Transport was hacked that October.[5] The Administrator of the Port of Lisbon was hacked last week, with criminals claiming to have stolen financials, audits, budgets, contracts, and ship logs.[6]

FBT Gibbons

A successful hack by a determined adversary, whether criminal or nation-state, can force a company to make large unplanned expenditures, lose business reputation, and anger vital partners. Then afterward it must comply with state privacy-disclosure laws, state and federal notification laws, and face risks of litigation.

Despite these pernicious threats, many transportation companies lack appreciation for the simple fact that the industry's business model requires cyber-interdependence among all components of its supply chains. And there is still a stubborn sentiment that cybersecurity is an IT problem when it's actually a corporate problem. In the modern environment, IT's involvement throughout the enterprise is just as critical to profits as vendor management, supply chain continuity, and physical security.

So what is a logistics company to do? Glad we asked… it should begin by presuming its networks will be successfully compromised. As fatalistic as that sounds, it simplifies the preparations necessary to overcome that calamity because the focus becomes "how do we recover if our key data is encrypted, our website and networks are down, and our most sensitive information is publicly disclosed?"

Cybersecurity is a people, procedures, and awareness problem.[7] Expensive security solutions won't succeed unless people working your supply chain practice good cyber-hygiene. Being transparent about good standards develops a business relationship with clear expectations. At a minimum these should cover training, network defenses, and response planning issues.

There are at least three fundamental steps for internal resilience: Identify and protect key IT assets; test network for weaknesses; maintain and exercise incident response plans. Unless executives and General Counsels appreciate which IT assets are most impactful to profits and operations, they may miscalculate when defending their networks.

This means the leaders primarily responsible for the use of a cyber asset should have an accountability role for its cybersecurity, which should then trigger the realistic conversations companies should have. It also means using vendors committed to building secure networks, in training your workforce, and understanding what to do

when hacked.

We suggest three similar steps for external resilience. Everyone in the supply chain needs to prioritize cyber-resilience; agree on security requirements with vendors and customers; and agree that all members of the supply chain will confidentially report significant cyber incidents within the group. These steps will require assistance from General Counsel or company lawyers but will be worth the effort.

Before approaching companies within your supply chain, you should have a working idea of what and where your risk is, where and how data is stored, and who has access to it. Review insurance coverages to ensure caps on limitation of liability and indemnification are within acceptable levels. These will prepare you to ask vendors or customers how they protect and store data. Asking them to meet your requirements can be made easier by relying on widely recommended standards, like NIST or CISA[8] standards, or ISO/IEC 27001.[9]

Finally, have a plan. CISA strongly recommends having an Incident Response Plan tailored to your company. That plan will make the first 48 hours of any attack much easier. You will know who gets involved, how and when, measures to quickly take without discussion, and have a communication plan in place.

This should set you up for resilience.

For more information, please contact any attorney with Frost Brown Todd's Supply Chain Service Team.

About the Author:

Frost Brown Todd Partner Gene Price has substantial real-world experience in cybersecurity and focuses on Frost Brown Todd's privacy and data security practice and incident response planning. Gene also represents clients regarding insurance and business claims, maritime matters, cybersecurity audits and certifications. Recently retired from the U.S. Navy as a Rear Admiral after 36 years of service, Gene served as Deputy Commander of Fleet Cyber Command/U.S. Tenth Fleet, where he supported U.S. Cyber

Command, the National Security Agency, and U.S. global cyber interests. He returned to fulltime work as a civilian in October 2022.

---

[1] Ransomware hackers are now going after supply chain companies (qz.com)
[2] US airport websites knocked offline by Russian-speaking hackers | The Hill
[3] Russian military behind October ransomware attacks on Ukraine, Poland
[4] Russian hackers targeting Dutch gas terminal: report | NL Times
[5] Ransomware hackers are now going after supply chain companies (qz.com)
[6] Hackers attack Port of Lisbon, threaten to leak stolen data, TRADEWINDS, 30 December 2022
[7] Paraphrase of National Institute of Standards and Technology Security (NIST) Principles
[8] Critical Infrastructure and Security Agency
[9] International Standards Organization/International Electrotechnical standard for information security management systems

FBT Gibbons