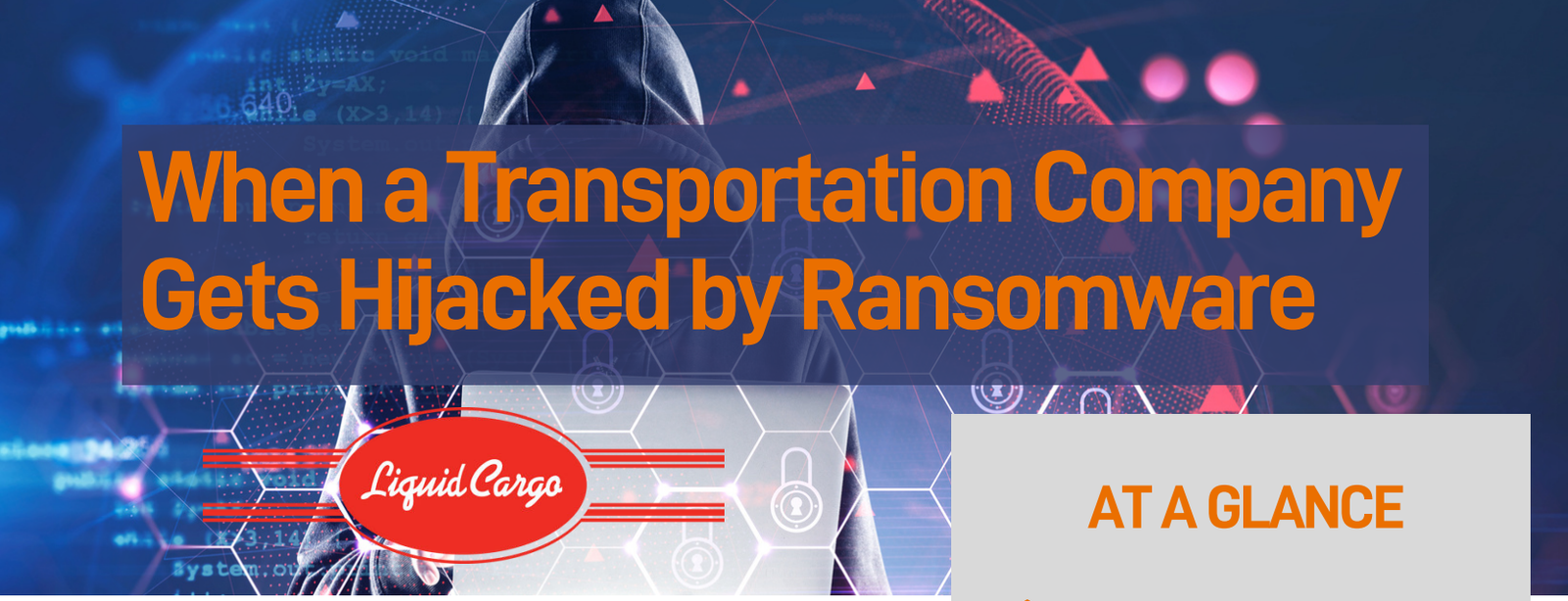

When a Transportation Company Gets Hijacked by Ransomware

Liquid Cargo is a renowned name in the USA and Canada in the ISO (International Organization for Standardization) Tank industry, already having 100 years of experience within the trucking industry. Kevin Jackson was traveling on the other side of the country on February 17, 2017, the start of the President's Day weekend, when Liquid Cargo was hit with a ransomware attack. He had little expectation of rapidly fixing the situation—or of enjoying his vacation—once he understood that he wasn't immune to a cyber-attack of this nature.

Ransomware cases like this one don't happen every day, but they happen often enough to show why it's so important to have a 360-degree IT solutions provider on your side. Kevin Jackson, CEO of Liquid Cargo, took the help of Protected Harbor, and his business has been on the upswing ever since.

AT A GLANCE

- 5 Bitcoins were paid as a ransom
- Operations halted for two weeks
- Servers had to be manually mounted and then moved piece by piece
- 3.5TB of data to be moved

THE PROBLEM

Liquid Cargo had contracted with an individual for IT assistance and security services at the time of the incident. Because the organization lacked sufficient security controls and procedures, hackers were able to access the network through a remote desktop protocol (RDP) connection. They gained access to the backup system through a backdoor, deleted all their files, encrypted the original ones, and notified Jackson of the situation.

Sadly, Jackson's experience isn't unique. "It's a common exploit," Luna said, "We're still using a shared model from the 1990s, so if a single person in a 10-person office clicked on the wrong thing and became infected, the whole office became infected. Now that it is a flat model and each computer can talk to another, they are all infected, and there is no guardrail, no layer of protection, and we are left with a mess to clean up."

> "It also changed how I think about business in an internet-connected world. It made me realize that there were some serious shortcomings in our security measures."
>
> **Kevin Jackson**
> **CEO Liquid Cargo, Inc.**

When Liquid Cargo first reached out to Protected Harbor for help, their data was stored on physical servers that were not running optimally due to a lack of maintenance. They had no way to access data remotely or from multiple locations at once – meaning there was only one person who was able to view files and make changes at any given time. Migrating Liquid Cargo's existing physical servers to a new virtual one also posed a challenge since the original servers were a mess and poorly managed. It was time-consuming as it had to be manually mounted and then moved piece by piece eliminating the unimportant information

PROTECTED HARBOR

THE SITUATION

Liquid Cargo was locked out of their data access, systems, and servers. This disrupted the bulk of their transportation and logistics operations for nearly two weeks. A ransom of five bitcoins was demanded to unlock the encrypted data, restore their systems, and return their business to normal-a nominal amount by today's standards.

First, he contacted the FBI, who advised him not to pay the ransom, which meant that the information wouldn't be retrieved. Unable to figure anything out, Jackson reached out to the hackers to scale their demand.

At the time, one bitcoin was worth $1,000. Jackson had some difficulty collecting those bitcoins, but he eventually did so, transferred the bitcoins to them, acquired the passcode, and then unencrypted the entire data and restored the systems. By the end of 2017, the value of the digital currency had surged, hitting $20,000.

THE SOLUTIONS

After Liquid Cargo was restored, Jackson's priority was to find a new 24x7 IT service and security supplier. "Any transition is challenging," he said, "but it was instantly evident how vital it is to work with a firm devoted to your security and safety rather than a person." His colleagues had connected him to Richard, who dug deep into his systems and advised Jackson that, "he needs a lot of help."

1. **Ensuring Clean Copies:** After a P2V (Physical to Virtual) attempt that failed due to a general system error and back-ups couldn't be created because they had no space, Protected Harbor decided to bring up VPN Tunnels from their office to Liquid Cargo and migrated their VM, so we had clean copies.

2. **Rebuild Servers:** We planned to do a slow piece-by-piece migration, server by server and rebuild them here, but, they were going to be hit by a tornado, so it was not doable. Jackson FedEx'd his physical server to Protected Harbor's office. Eventually, we spent more time band-aided them to do it gradually rather than just ripping it off. So our spent the whole weekend completing the migration.

3. **Email Migration:** Emails were over a Terabyte alone! Built out environment based on core apps Debo Pro, TMS, and old access applications. But those apps had access and connections to other databases and apps to pull data. Protected Harbor spent 2 weeks cutting over and redoing application connections.

4. **Proactive Security:** Protected Harbor detects and reacts to threats more rapidly by building its systems. For example, Liquid Cargo is alerted within minutes of a phishing email or if someone opened a suspicious email link. That's fast enough that we can be more proactive because ransomware needs time to percolate, ferret out files, and figure out where everything is.

5. **Modular Design:** We make your company fits into our modular design. You get a small piece of infrastructure. You get benefits from whole but have your own little corner. At its center, the core design does not change nor does the process. Protected Harbor hosts “clusters” of computers with dedicated servers for individual clients. If one computer, or “node,” in the cluster fails, it shuts down, and the next one boots up. “Kevin's dedicated server is ‘virtual,’ meaning he doesn't have a physical box anymore,” So if somebody tries to attack it, the virus doesn't understand where it is because there's no disc to go after, and there's no CPU to attack.

PROTECTED HARBOR

THE RESULTS

Liquid Cargo's existing physical servers with 3.5TB of data were transferred to a new virtual server. Richard Luna, along with a team of tech-savvy software engineers and IT professionals, is focused on providing complete, unrivaled IT solutions that leverage technology as an asset rather than an expensive distraction. Starting from single physical server infrastructure, they now have 9 virtual servers in their dedicated network, which can expertly handle any work- load. Following the migration, Liquid Cargo saw a 100% increase in efficiency.

During the move, Liquid Cargo hired a third-party VoIP services provider who still managed the SIP phones. Their phone servers were also moved to Protected Harbor's office and plugged in after they complained about the poor service. A whole year later, we launched a new VoIP system as a solution, a video conferencing and messaging system, removing Liquid Cargo's troubles for good.

“But having now seen what we had vs. what we have now, I believe it. Working with TBs of data and ugly physical servers, I saw a 100% increase in efficiency.” Jackson said, responding to the quality of services before and after migration.