The Facts on LTL and Dimensional Shipping
Continued from page 20

to move, but they may not offer it unless they are asked. Before you begin, know two important things: 1) the customer, and 2) the truckload rates. Next, determine truckload cost to carrier for that lane. You can prorate a partial shipment as a percent of a truckload shipment rate to carrier. For example, one-quarter of a truckload would equal 50 percent of a truckload rate to customer, one-half truckload would equal 75 percent of a truckload rate to customer, and three-quarters of a truckload would equal 95 percent of a truckload rate to customer.

When speaking and negotiating with carriers, make sure to ask the right questions, such as: Is there any space left on the trailer, what is the delivery date/time and pick up date/time. Keep in mind that partials are covered by truckload carriers. It is also important to note that carriers will not always know the room they have left until late in the day, so do not give up too early!

Partial truckload shipping is a value-added service which makes this is a great way to help differentiate you from the competition because most freight brokers overlook them. So, start tapping into your carrier network, access trailers that have extra space and never pay full truckload rates to move less freight again!

When should you consider shipping Partial Truckload?

- If you ship 3,000 pounds or more using an LTL common carrier.
- If your freight is light or takes up a lot of space.
- If you find it cheaper to send a full truckload than to send 5,000 pounds.
- If you ship 10 or more pallets as a full truckload.

What are the advantages of shipping Partial vs LTL?

- Partial Truckload (or Load to Ride) ships your freight directly as soon as it is loaded.
- There is a lower risk of damage, with less handling.
- There are lower prices than LTL or Truckload.
- Transit times are generally faster than LTL due to the lack of re-handling

Please know that the above information provided serves only as a basic introduction to Less-Than-Truckload (LTL) (and partial truckload) freight shipping. Many important factors come into play when deciding to ship LTL as opposed to other services. If you are a freight broker agent that is unfamiliar with shipping LTL, please make sure to obtain proper training and fully educate yourself before launching into this endeavor. An error on your part could mean an increase in freight charges or even worse, losing credibility to your customer.

Protecting 3PL and Trucking Companies Against the Growing Threat of Ransomware

By Chuck Cook

Ransomware is a particularly vicious kind of malware that has existed for several years. Recently, both the number and sophistication of ransomware attacks are escalating. Not only does ransomware capture information and wreak havoc with IT systems, it also steals the victim's money through cyber-extortion. Hackers are able to break into a system, encrypt the data it contains to prevent its use, and then demand payment to release the data.

Ransomware attackers first preyed on individuals by hacking into their personal systems and paralyzing the data until payment was made. Attacks were, and often still are, random rather than targeted. Hackers have since shifted their focus away from private citizens and instead focused on corporations. Why? Because if individuals are willing to pay several hundred dollars in bitcoins to recover their data, then surely corporations will pay much, much more.

This is especially dangerous for businesses that rely not just on great masses of critical data, but also on a rapid and continuous flow of that data. As a result, 3PL and trucking companies are high on the list of vulnerable organizations.

Once ransomware infects a network, it encrypts any and all data that the network has permission to access, including system files and backup storage. When an infection takes hold, a window may pop up or a folder labeled something like "decrypt help" may be created. This window or help folder says that the files will be returned if the victim

Continued on page 25

Protecting 3PL and Trucking Companies Against the Growing Threat of Ransomware
Continued from page 22

pays a ransom. Of course, there is no guarantee that the data will be restored and there is a risk that further ransom demands may follow. A ransom attack can quickly become a data disaster that takes days to remediate and restore.

Although servers incur the most damage, intrusions usually come via PC workstations and laptops connected to the network. While hackers are in control, management and staff cannot utilize their email applications and must rely instead on fax, phone, or face-to-face communication. Employees cannot access records in a timely manner and are thus unable to proceed with business until the relevant data is available.

> At first glance, everything may appear normal while, out-of-sight, an executable program is encrypting files.

Ransom payment demands are often ridiculously exorbitant and can be bargained down. Demands and payments range from perhaps from millions to tens of thousands. These financial losses are substantial and can severely damage a company's business operations, reputation, and even market share.

All it takes is for one employee to open a seemingly harmless, everyday email with an attachment. At first glance, everything may appear normal while, out-of-sight, an executable program is encrypting files. The only way to get the key to unlock the encryption is to pay the ransom. Some variants infect environments without clicking, by exploiting unpatched systems or insufficient security.

Ransomware is especially threatening to environments such as those of 3PLs and trucking companies in which voluminous transactions and communications are flowing constantly and people work at a fast pace. This makes it easier for employees to be tricked into opening and interacting with bogus emails.

So what can 3PLs and trucking companies do when they are attacked by ransomware, if a strong protection program has not yet been implemented?

Don't pay the ransom. If you do, the crooks have no incentive to let you off the hook. If you give in to threats, then you can expect more demands with no guarantee of a good outcome. Even if the hackers are satisfied with one payment, they have no incentive not to strike again.

If possible, find out which strain of ransomware you are up against. Hackers work constantly to develop new weapons and counter the latest safeguards, so it is well worth the effort to find accurate information about your particular intrusion.

Isolate the infected systems. Removing infected machines from your network may leave you temporarily hobbled, but the threat will be contained and you can get to work on removing the ransomware.

What can you do to effectively and reliably guard against ransomware? Follow these key steps:

Establish a company policy and get everyone involved. Educate employees about the risk of clicking on unknown links. This is imperative for avoiding ransomware attacks, but this is only part of the picture. As a matter of policy, prohibit users from clicking on unverified email links from any unknown source unless authorized by a manager or your IT department.

Upgrade your security. Install latest-generation endpoint protection software to stop viruses and malware at the PC or laptop level before infection occurs. Incorporate an email filtering solution to block known viruses and malware before users have a chance to click on them.

Always have a latest-generation firewall in place. In addition, consider a security monitoring service.

Upgrade your backup tools. Evaluate your Data Backup solution and be sure you have multiple-version roll-back capability. Some malware corrupts the OS files, so in addition to Data Backup, install a Server Recovery Solution that captures a snapshot of the entire server image for rapid server recovery. Consider a High Availability Solution. This will enable you to recover in minutes.

Check your backup emails regularly. Each morning, someone at your company should get an email notification from your backup system. If the email contains an error message, forward it to your vendor for verification. Error messages can help identify file system problems caused by malware.

This is not the whole picture, of course, but simply an outline of the dangers of ransomware and the steps that 3PLs and trucking companies should take to protect against the threat and to be able to rebound quickly when an attack occurs. Be aware that, just as each organization's IT footprint is different, so too is the company's ideal plan for guarding against ransomware.

For more information on overall data and systems protection for 3PL and Trucking Companies, please reference RenovoData's website at www.renovodata.com or call 1.877.834.3684.