Essential Cyber Lessons to Mitigate Risk for Your 3PL

Charles "Chuck" Cook | RENOVODATA

ADOBE STOCK/PARRADEE

Enhance Your Cyber Posture Today

The transportation industry is under siege. Bad actors have identified 3PLs as a vertical that is reliant on their IT infrastructure and have zero tolerance for operational downtime – making them especially susceptible to ransomware and other cyberattacks. The severity and frequency of cyberattacks continues to grow year over year. Here are some statistics from this past year alone.

- The average cost of ransomware event in 2023 was $1.54 million, double the 2022 average.
- Ransomware payments exceeded $1 billion in 2023.
- 50% of ransomware attacks globally are on U.S. organizations.

Fortunately, cultivating a defense against cyber-attacks has become a more attainable goal. Cybersecurity frameworks, disaster recovery solutions, and skilled partners are all available to organizations who are willing and ready to make investments in their organization and their culture. The following 7 Cyber-lessons are guaranteed to modernize your 3PLs Cyber Security Posture.

Build a Strategy and Culture of Cybersecurity

Regardless of the investments already made in an organization's IT department, it's easy for cybersecurity to fall by the wayside. An IT strategy that brings operational excellence is always the primary concern, but without adequate defense, the infrastructure can fall like a house of cards.

Adopt frameworks like NIST, IS027001 or CIS Controls to provide structured guidance for managing and reducing risks. The first step in building cyber posture across your organization is to approach cyberthreats as a business risk – not just an IT risk. To effectively manage these risks, it is crucial to raise awareness and reinforce a strong security culture at all levels of the organization. Understanding the cost of prevention is key, as neglecting cybersecurity can lead to significant financial and reputational damage. Establishing a dedicated team and budget ensures that resources are allocated appropriately to combat threats. Implementing company-wide cybersecurity policies further solidifies the organization's commitment to safeguarding its digital assets and maintaining a robust security posture.

Document and Categorize IT Assets

Half the battle of addressing the cyber-risks your 3PL is facing is knowing what you have, and the threat vectors those assets present. Start by documenting software assets – including all your applications that have access to the company network and store organizational data. Then, continue the documentation by listing all the hardware assets that support your organization's information technology. This might include servers, physical firewalls, datacenters, modems, routers and Cloud Service Providers. All these physical and virtual assets need to be categorized by their criticality – where the most critical assets get the most budget for security solutions and services. Furthermore, ask the team, how long can your company manage to be without these critical assets? Then you can establish recovery and retention objectives that are congruent with the needs of your systems and data.

Protect & Monitor Your Network

Most data breaches and cyber-attacks are attributed to human error. This is a testament to the concept that "not every employee needs access to everything". Fundamentally, you need to limit user access based on needs, across departments. On top of user access, all servers and PCs that touch the company network need to have adept malware protection tools and software that can catch viruses that can propagate with a click of the mouse. Another threat vector that is commonly ignored is the degradation of the operating systems which servers run on. They need frequent updates to patch common attack opportunities. These servers and networks should have tools that monitor log files for any changes that are being made as a bad actor gears up for an attack. A great way to evaluate the protection protocols and defense your organization has in place is to engage a 3rd party to conduct a vulnerability test. This evaluation will outline any points of access and other items that still need to be addressed.

Build Cybersecurity Awareness & Vigilance

It's the responsibility of management and IT leaders to create guidelines, adopt frameworks, and promote good IT behavior within a company. Policies such as "Acceptable Use" & "Termination" are two sets of guidelines that spell out for an employee how they are permitted to interact with company data, systems, and the network. IT managers are always pressed for resources, that's why it's suggested that a company looks to cybersecurity training providers to help further bolster cyber posture. Training needs to be ongoing and simple. They often include short videos, quizzes, and faux phishing tests that take a wholesome approach to making the average user more adept at identifying threats. There is constant news about data breaches, new threats, and financial loss incurred by companies infected. Sharing this information from time to time is a great way to keep employees reminded of the risks. Employees are often the weakest link in cybersecurity and financial loss can be incurred by companies infected. Staying vigilant about current data breach threats and the importance of new security policies will ensure your company is positioned well.

Maximize Your Backup & Recovery Capabilities

Unfortunately, no matter the investment into preventative capabilities of users, servers, and networks – something will always slip through the cracks. That's why backup and recovery are a vital layer of any organization's cybersecurity. Backup and recovery should always be on constant evaluation for any additions or changes that have been made to infrastructure, and tested frequently to ensure recovery objectives are being met. The most secure backups for critical data are air-gapped and encrypted, providing additional security even if a bad actor were able to gain access to the company network. Each recovery test that is conducted should be documented thoroughly with any observations or lessons learned that can be addressed to make recovery even more efficient over time.

Invest in Trusted Vendors & Partnerships

Service providers that are adept in cyber-training, backup and recovery, or IT support will give IT managers ample resources to lean on when a disaster strikes. Information sharing between a provider and an organization is vital. For example, a provider may have more access to recent data about cyberthreats that are targeting the transportation industry. When the minds of internal and external IT professionals can collaborate and form a team, this provides a mix of backgrounds and competencies that can better protect an organization. However, the support provided is only as good as their availability in a disaster. Know who to call, text, or email when worst comes to worst.

Plan and Insure for the Worst

The connective tissue between documenting assets, training employees, backup and recovery, and having providers you can trust is an organizations' disaster recovery plan. This comprehensive plan outlines plainly what data, tools, systems, networks, and people are involved in ensuring swift recovery of an organizations' operations. A DR plan coupled with communications policies that outline who needs to be notified of an attack or natural disaster demystify how to recover even when chaos is ensuing. Regularly evaluate your cybersecurity posture through audits and assessments. This helps identify vulnerabilities, assessing the effectiveness of current measures, and making information decisions on necessary improvements. The final piece of recovery is minimizing the financial risk involved with suffering a disaster, and that's where insurance comes in. Cyber-insurance coverage has grown significantly over the years, but many of these providers now require a disaster recovery plan for you to be able to meet their tiered coverage. Make sure your plan is comprehensive enough to be useful internally and meet external requirements that help cover financial responsibility during a disaster event.

You Make the Difference

Ultimately, you and your organization's IT leadership make the difference in ensuring a robust cyber-security posture for your organization - by driving cybersecurity strategy, investment, and culture. Inventory and protect critical assets and applications thoroughly. Audit and limit network access internally and externally. Develop your team's readiness – build security awareness and vigilance through ongoing training. Upgrade your backups to avoid data loss and maintain critical operations. Establish a group of trusted partners and vendors that can enhance security and assist in disaster scenarios.

By investing in these areas and integrating them into a comprehensive disaster recovery plan, your organization will be well-prepared to handle cybersecurity incidents and mitigate the associated risks. Cyber insurance acts as a final safeguard providing financial coverage when all other measures are exhausted, ensuring your company's long-term resilience and stability.

RenovoData is a leading cloud backup, Disaster Recovery, Infrastructure as a Service (IaaS), and DR Planning service provider helping companies protect critical data and systems worldwide. For more information and guidance, please call toll-free at 877-834-3684, email us at info@renovodata.com, or reference our website at www.renovodata.com

GETTY IMAGES/METAMORWORKS