

Fight Ransomware with Cyber Resiliency

Chuck Cook | RENOVDATA



TRANSPORTATION ORGANIZATIONS ARE not only at a higher risk of fallout from ransomware due to their 24/7 uptime requirements, but studies also show that transportation is targeted more frequently than other industries. When ransomware infiltrates your network, it can spread horizontally and vertically through your infrastructure like wildfire, garnering administrative credentials and encrypting all the IT systems and data in its wake. In some of the worst cases, operations stop immediately; normal business functions like booking loads and even sending emails could take anywhere from hours to weeks to restore. Depending on the ransomware variant, and how long it laid dormant in your environment before it was activated, a complete infrastructure rebuild may be necessary and could take weeks or months to complete.

THE DEMANDS VARY IN **BOUNTY SIZE** AND CURRENCY, BUT IF YOUR **RECOVERY METHODS** ARE NOT WELL **ESTABLISHED AND EVALUATED**, YOUR ORGANIZATION'S FIRST RESPONDERS WILL BE **RIDDLED WITH PANIC**.



Ransomware is a global threat. The war in Ukraine alongside continued aggression from countries like North Korea and Iran has shown a breadth of complex ransomware and other cyberattacks. Terrorist operations like this—state-led or otherwise—target sectors such as government, finance, and transportation to create mass hysteria, disrupt the domestic industry and harm people.

The demands vary in bounty size and currency, but if your recovery methods are not well established and evaluated, your organization's first responders will be riddled with panic. The compulsion to pay can be overwhelming. Unfortunately, criminals are not often honest, and there is no guarantee that payment will pave the way to restoration. It is more likely that your organization's name is marked in a database of targets who are willing to pay.

Ransomware Today:

- In 2021, ransomware attacks increased 93% year over year. (Check Point)
- The total, global, cost of ransomware in 2021 increased to \$20 billion. (Cloudwards)
- In 2021, the average cost for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. was \$1.85 million. (Sophos)
- 37% of global organizations surveyed by Sophos said they were victims of a ransomware attack in 2021.
- SonicWall's 2022 Cyber Threat Report addresses multiple examples of ransomware growing in the transportation industry. This includes a case of an established ransomware gang using UPS and United States Postal Service to snail-mail USB Drives in packaging that seemed to be from Amazon or the U.S. Department of Health. These USB drives were lethal to systems, and the gang specifically targeted organizations in defense, insurance and transportation.
- The Transportation Security Administration introduced cybersecurity requirements for transportation critical infrastructure—currently including high-risk freight, passenger rail, and rail transit—the directives require owners and operators to designate a cybersecurity coordinator, report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours, develop and implement an incident response plan, and complete vulnerability assessments.

There are numerous internal and external factors that determine an organization's cybersecurity resilience. Staff, information systems, physical environment, and insurance are just a few examples of organizational elements that need fortification. Ransomware is here to stay—developing cyber resilience



is a task that cannot be neglected. Stifle ransomware infections through preventative tactics such as protecting your endpoints, training your employees, and backing up your data. Avoid paying the ransom by enhancing your recovery strategy with a secure disaster recovery site, rapid recovery software, cyber insurance, etc.

Interconnected Protection

The individual risk vectors threatening your IT environment all have different tools that could mitigate the risk and help fortification efforts. That's why it's important to acknowledge the interconnectedness of both the cybersecurity tools and processes used to protect your environment. For example, to bolster your recovery readiness you'll certainly need a disaster recovery plan, but components needed for an effective plan include secure data backups to restore from and a place to restore to in case of an entire site outage. Even more granularly, your data backups and Disaster Recovery (DR) site will need to be protected, scanned for vulnerabilities, patched and updated, and tested regularly for quality assurance. The more you invest in each risk vector, the more cyber-resilient you become.

A beneficial framework for 3PL and trucking companies to consult is the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, a document that gives organizations of all sizes a set of guidelines to help evaluate and manage their cybersecurity risk. The functions of the *Framework Core* aid an organization in managing risk by organizing the information, enabling decision-making, addressing threats, and constantly improving and testing the resilience of the environment. These functions are Identify, Protect, Detect, Respond, and Recover. The functions, like the aforementioned solutions, are interconnected, sequential, and have a constant requirement to be updated and evolved. The NIST Framework¹ is exhaustive in its cybersecurity considerations, and it's an effective resource for organizations at all levels of resilience to consult when recovery planning.

Endpoint & Personnel Protection

There are plenty of defenses an organization can do to enhance their network. Network protections such as secure Virtual Private Networks (VPN's), next-generation firewalls (NGFW), anti-virus, and multi-factor authentication prevent your organization from becoming an easy target to infect. Ensure your infrastructure—especially firewalls—are updated. Older technology is more vulnerable to breaking down, becoming obsolete, and having security exploits developed against it. Whether it is an infrastructural level intrusion, or it simply came from a toxic click in an email, it's important to invest in addressing these vulnerabilities.

Physical and virtual machines take the brunt of the damage with corrupt systems and lost data, but ransomware attacks most commonly weave their way into an organization's IT environment starting at employee workstations. Establishing policies (such as Acceptable Use, Internet Use, and Password) and plans (including DR and Business Continuity) can empower your employees with tools and procedures. Workers with a lower technical aptitude, or those in a department unrelated to information systems, are the employees that most deserve an opportunity to educate themselves on how to protect data and how to avoid making costly mistakes. Cybersecurity training for employees is a low-cost, high-yield risk mitigation tool. Even basic training programs on topics, such as *How to deal with phishing emails*, have shown as much as a 7-fold return on investment. Moving back into hardware, corporate standards for endpoint protection, including the anti-malware and data backup solutions, should be installed on every device that is connected to the company network. Additionally, tools like email message continuity and filtering should be implemented to mitigate phishing attacks, and to protect valuable data in email.

Backups ≠ Recovery

The more protections you implement, the more you minimize your risk. Data backup plays an essential role in disaster recovery, but a blend of services, solutions, and planning will help complete the goal of cyber resiliency. Sometimes, mixing, and matching solutions depending on your organization's Recovery Time Objective (RTO—how quickly an organization needs to be back online after an outage) and Recovery Point Objective (RPO—what point in time your organization would like to restore) can help accomplish these goals. Ideally, both backup and recovery solutions are selected depending on your RTO/RPO and the nature of your IT environment. Fine-tuning your strategies and aligning them with your solutions is key to minimizing downtime and risk.

Data Backup Options

Don't be surprised to find you need multiple tools in order to accomplish your objectives. When shopping for backup tools, consider solutions that offer different layers of protection such as OS-level backups, database backups, and file sync and share options. All these different breeds of backups serve different purposes and vary widely in investment—but it is worthwhile to spend

EVERY SO OFTEN, EVEN THE **MOST FORTIFIED ENVIRONMENTS** ARE SUBJECT TO A **RANSOMWARE ATTACK**, AND IT'S USUALLY BECAUSE OF **HUMAN ERROR** OR AN **INFRASTRUCTURE-LEVEL VULNERABILITY** COMPLETELY OUT OF THEIR CONTROL.

time carefully researching and speaking directly with subject matter experts to find which is right for your use case. Operating System-level backups, also known as snapshot technology, are one of the most popular and effective backup solutions available. They allow you to store multiple versions of your entire system state. This grants access to the blueprint to rebuild your server from scratch, given the availability of replacement hardware or a hosting environment. Then you'll need to establish a retention policy depending on both your needs and your budget. The more robust your data retention plan, the more you can expect to pay in cloud storage costs.


Disaster Recovery Options

Disaster Recovery is different from data backup because you have a pre-determined environment for recovery if your primary environment is impacted from a data loss event. Premiere disaster recovery tools offer features such as log-based replication for continuous data protection. The solution works similarly to a DVR, allowing administrators to rewind their servers to a point-in-time before the ransomware infection struck. If the solution has been tested and validated—the fear of having to a pay ransom or recreate lost work should be significantly reduced. A planned and implemented DR solution can recover corrupt applications and data nearly instantly compared to traditional backup.

Beyond software, it's often wise to invest in dedicated recovery equipment. If your IT department has dedicated equipment and storage with the sole purpose of storing backups onsite, there is peace of mind in having an immediate fallback option. If equipped properly, this solution can provide the ability to boot up server clones until your primary systems are restored or replaced. The result is rapid recovery from hardware failure with dramatically reduced downtime.

Become Cyber Resilient Now

Ransomware gangs globally are becoming more sophisticated in their structure and the methods of delivering malware, with no sign of slowing. Every so often, even the most fortified environments are subject to a ransomware attack, and it's usually because of human error or an infrastructure-level vulnerability completely out of their control. Those who are not well protected should invest—even further—in the ability to recover data and restore business continuity, especially if it has been some time since the investment has been tested,

updated, or maintained. Utilizing a combination of the best software, hardware, and service providers at your disposal is core to ransomware resiliency. Don't pay the ransom. Instead, leverage essential tools and standards to build a culture of cyber readiness. Do your organization a favor—get out in front of it by investing in cyber-essentials before it is too late. 

RenovoData is a leading cloud backup and disaster recovery planning company, and DR/BC planning service provider helping companies protect and restore critical data worldwide. For more information and guidance, please call toll-free at 877-834-3684 or email us at info@renovodata.com.

Reference

¹NIST Framework. <https://www.nist.gov/cyberframework>



**Best Lawyers
LAW FIRM
OF THE YEAR
USNews
TRANSPORTATION LAW
2022**

100+ FREIGHT INTERMEDIARIES CAN'T BE WRONG

Over the years, Benesch has provided legal consultation and pragmatic business advice to well over 100 Transportation Brokers, Surface Freight Forwarders, Ocean Freight Forwarders, NVOCC's, Air Freight Forwarders, Warehousemen, 3PLs, 4PLs, and other Freight Intermediaries of all kinds. They know that when it comes to corporate structuring, mergers and acquisitions, transportation and logistics contracts, best practices, regulatory challenges, insurance and risk management, freight loss and damage or freight charge disputes, catastrophic personal injuries, and independent contractor relationships — **Benesch knows Intermediaries.**

Benesch Counsel for the Road Ahead®

*Benesch received the distinction of being named **Transportation Law Firm of the Year** by Best Lawyers®—Best Law Firms in 2022, 2020, 2017, 2016 and 2014. Only one law firm per practice area in the U.S. receives this recognition each year, making this award a particularly significant achievement.*

www.beneschlaw.com