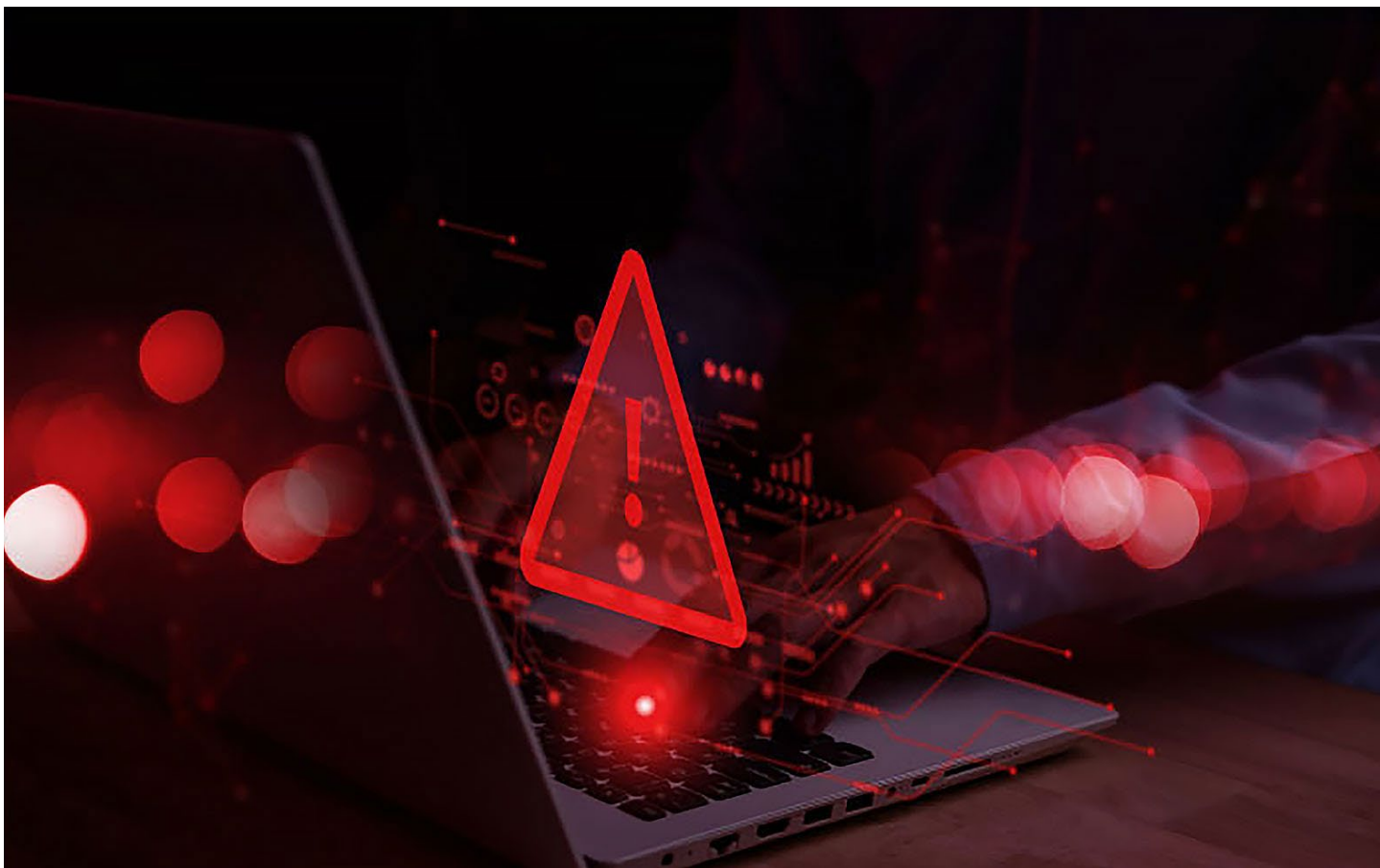




By Chuck Cook, President of RenovoData
October, 2026 – 3PL Perspectives

3PLPERSPECTIVES

Cyberthreats Travel Fast. Can your Business Recover Fast Enough?

CYBERSECURITY HAS LONG BEEN VIEWED AS a game of prevention. Organizations invest heavily in firewalls, endpoint protection, email filtering, identity management, and employee awareness training with the goal of keeping attackers out. While prevention remains essential, today's threat landscape demands a recovery-focused perspective.

Cybercriminals have become faster, more sophisticated, and increasingly powered by artificial intelligence. Even 3PL's with mature security programs can fall victim to ransomware, phishing campaigns, software vulnerabilities, or supply chain attacks. The question is no longer whether an attack will occur, it's how quickly your business can recover when it does. The organizations that can recover in hours instead of days don't have better cybersecurity, they have better recovery strategies.

The New Reality of Cyber Threats

Artificial intelligence has fundamentally changed how threat actors operate. Tasks that once required days or weeks of manual effort can now be completed automatically in a matter of minutes. AI enables attackers to identify vulnerable systems, craft convincing phishing emails, and move laterally through compromised environments with remarkable speed. This acceleration has real business consequences.

Recent industry reports indicate:

- Ransomware activity increased significantly in 2025 compared to the previous year.
- AI assisted attacks have become commonplace across ransomware campaigns.
- Logistics and transportation organizations continue to experience increasing growing operational disruptions caused by both cyberattacks and cargo theft.
- Nearly half of organizations still lack a tested disaster recovery plan.
- These trends illustrate an uncomfortable truth. While attacks continue to accelerate, many organizations haven't improved their ability to recover. That imbalance creates unnecessary business risks.

How AI is Accelerating Cyberattacks

Artificial intelligence isn't just making cyberattacks more common, it is making them dramatically more efficient. Modern ransomware groups leverage AI to automate many stages of an attack, including:

Automated Reconnaissance

Instead of manually researching an organization, AI can rapidly scan cloud environments, warehouse management systems (WMS), transportation management systems (TMS), IoT devices, and publicly exposed services to identify weaknesses.

Smarter Phishing Campaigns

Generic phishing emails are giving way to personalized, highly convincing messages tailored to individual employees. AI can mimic writing styles, generate believable business communications, and reduce many of the grammatical errors that previously made phishing attempts easier to identify.

Faster Lateral Movement

Once attackers gain an initial foothold, AI helps identify privileged accounts, vulnerable applications, and critical infrastructure that can accelerate the spread of malware throughout an environment.

Better Timing

Rather than launching attacks randomly, cybercriminals increasingly time their operations around holidays, weekends, financial reporting periods, or other moments when organizations may have reduced staffing or heightened operational pressure.

The result is simple: attackers are becoming faster. Organizations need their recovery capabilities to become even faster too.

Prevention Alone Is No Longer Enough

Security technologies remain a critical first line of defense. Organizations continue to invest in firewalls, endpoint protection, identity and access management, application security, and employee awareness training to reduce their attack surface. These controls are essential in reducing risk.

However, these security controls don't eliminate risk, they can only reduce it. Eventually, every organization must answer a different question. If our defenses fail tomorrow, how quickly could we restore operations? Many organizations discover they don't know. Recovery planning deserves the

same level of executive attention as cybersecurity threat prevention because business continuity depends on both.

Understanding Recovery Readiness

Recovery maturity doesn't happen overnight. It evolves as organizations strengthen their processes, technologies, and testing. Many businesses begin at a reactive stage where backups exist, recovery procedures remain undocumented and largely untested. While backups provide some protection, there is often little confidence they will restore critical systems within acceptable timeframes.

As organizations mature, they begin documenting recovery procedures, defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), mapping application dependencies, prioritizing critical business systems, and verifying backup integrity.

The next step towards resilience introduces automation. Recovery processes become policy-driven, testing becomes routine, and infrastructure is designed with disaster recovery in mind rather than added as an afterthought. The most resilient organizations build dedicated recovery environments, leverage real-time replication, automate snapshots, and validate recovery through recurring disaster recovery exercises. At this level, recovery becomes a measurable business capability instead of an optimistic assumption.

Recovery Must Be Proven, Not Assumed

Many organizations mistakenly use the terms Backups or (BaaS) and Disaster Recovery (DRaaS) interchangeably, but they serve different purposes. A backup is simply a copy of your data. Disaster Recovery is the comprehensive strategy, technology, and processes required to restore entire business operations after a disruption.

Backups help protect data from loss, but they do not automatically restore applications, servers, network, connectivity, user access, or business workflows. Disaster Recovery focuses on recovering the complete IT environment, including the order in which systems are restored, application dependencies, recovery priorities, and the people and procedures required to bring operations back online.

Regular testing helps uncover issues long before they become costly outages. Recovery testing exercises can reveal corrupted backup data, undocumented application dependencies, outdated documentation, infrastructure changes that were never incorporated into the disaster recovery plan, or recovery times that fall well outside business expectations. Finding these problems during a scheduled test is far less expensive than discovering them during a ransomware incident.

Testing also provides an opportunity to validate more than just the data itself. It confirms that applications function properly after restoration, users can authenticate successfully, network connectivity has been restored, and critical business workflows operate as expected. Testing frequently uncovers issues that would otherwise remain hidden until an actual disaster.

AI Can Strengthen Your Defense, Too

Fortunately, artificial intelligence isn't just benefiting attackers. 3PL's can leverage AI throughout their own cybersecurity and disaster recovery strategies.

Modern security and backup platforms increasingly use AI to identify abnormal behavior, detect ransomware earlier, and monitor backup environments for suspicious activity before significant damage occurs. Behavioral analytics can recognize subtle indicators of compromise that traditional rule-based systems may overlook, giving security teams valuable time to respond before an incident escalates.

AI also enhances employee awareness by identifying suspicious communications and helping security teams respond more efficiently. Used responsibly, AI becomes a force multiplier for defenders.

Recovery Is a Business Strategy

Disaster recovery is often viewed as an IT responsibility. In reality, it's a business continuity strategy. Effective recovery planning requires collaboration across departments to determine which applications are truly mission-critical, how much downtime is acceptable, which business processes must be restored first, how internal and external communications will occur during an incident, and who is the purveyor of recovery decisions.

Technology enables recovery, but leadership defines recovery priorities. When business leaders and IT teams align with recovery objectives, organizations can make smarter investments and recover with greater confidence.

Build Confidence Before Disaster Strikes

Cyber threats will continue evolving. Artificial intelligence will continue accelerating attacks. No technology can eliminate every risk. What organizations can control is their level of preparedness. Businesses that recover fast share several common characteristics, such as maintaining verified backups, regularly testing disaster recovery procedures, defining clear recovery objectives, automating where possible, and finally, continuously improving after every test or infrastructure change.

Organizations that treat disaster recovery as a continuous process rather than an annual checklist are better positioned to minimize downtime, protect revenue, preserve customer trust, and maintain business continuity when cyber incidents occur. Disaster recovery success is measured by how confidently and how quickly you recover.