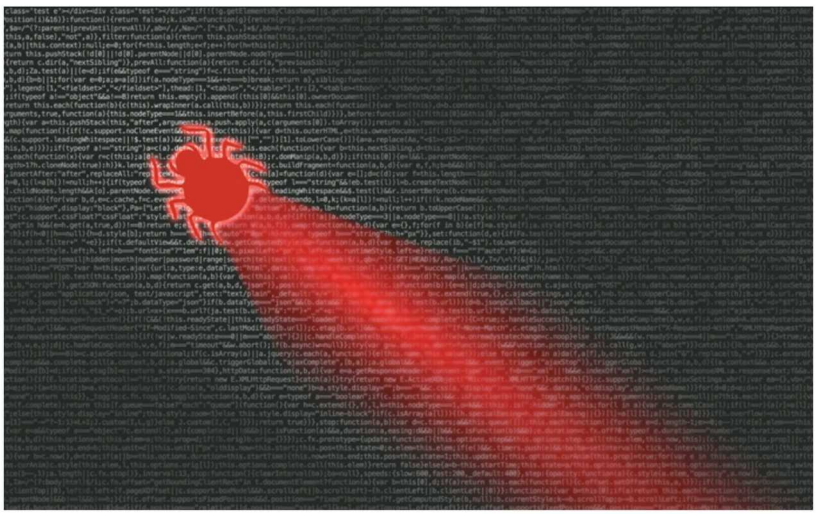
Know Your Security Vulnerabilities:

The Danger Is in the Details

Chuck Cook | RENOVODATA

WHEN DEVISING IT security processes or reassessing existing ones, 3PL and trucking companies should be aware of how many aspects need to be covered and how complex they can be. Vulnerabilities can be both external and internal, and serious perils can arise at many points.



ISTOCK.COM/BEEBRIGHT

Understand Why Systems Fail

Cybercriminals use many types of assault weapons, all of them craftily designed to avoid detection, so up-to-date armor is required to block as many kinds as possible. Hot targets include email, current and archived data, backup functions and applications.

Although malware, cyberthreats, and ransomware are the greatest risks 3PL and trucking companies face, and the ones we are most aware of, they are not the only perils. Others include employee sabotage, weather events such as hurricanes and floods, highway and railroad accidents, earthquakes, utility failures, IT shutdowns, power outages, roof leaks, and other physical plant problems, and last but far from least, fires.

Protect Against Internal Threats

Problems originating outside the organization are the ones that get the most attention, but those that wreak havoc from within are equally dangerous and can be harder to spot. These can include faulty, outdated, or poorly maintained equipment; ill-chosen software; or unwise corporate policies. But it's the risks that involve your team that can arise from honest errors, inefficient security practices, and deliberate sabotage.

The most effective protection against all three is regular companywide training coupled with stringent policies to prevent mistakes and destructive behaviors.

Set Internal Security Policies & Communicate Them Clearly

A central concern is preventing the introduction of unwanted software into company systems, and that means erecting stout barriers:

- Restrict access to specific data, networks, software, and other IT functions.
- Inventory your data, systems and applications.
- Prioritize the importance of all elements.
- Determine how long critical parts could be out of service before operations would cease.
- Establish clear rules for handling and managing data.
- Install and maintain malware filters for company email and websites.
- Bar the use of personal email accounts on company networks.
- Allow no personal or other outside devices entry into company networks.
- Secure all user accounts.
- Lock login entry after five unsuccessful attempts.

ISTOCK.COM/1001LOVE

Implement a Tough Password Policy

Passwords play a central role in strengthening internal networks. Here are some pointers for building safeguards:

- Use strong and unique passwords for each system, website, network and service.
- Longer is better.
- Use special characters along with letters and numbers.
- Employ password management tools.
- Schedule password changes.
- Demand that your people keep their passwords secret.
- Password-protect all devices that touch your system, including laptops, smartphones and other data endpoints.

Install Software Updates Promptly

New releases solve software and security problems and improve antivirus capabilities, so they should be implemented at once. Automate the update process and always register all versions of all the packages your company uses.

Train Everyone

The best possible defenses against security threats will fail if your staff is not actively involved. That means solid training for everyone who has a stake in data security, with the objective of promoting quick reactions to hazards:

- Training should not be limited to external threats; alert everyone to the possibilities of internal technical glitches and potential problems resulting from human behavior.
- Your people should understand current varieties of malware, be able to spot them, and know what to do when they are detected.
- Everyone should be trained to never click on "iffy" links.
- Establish action assignments for everyone to perform in emergencies.
- Promote ongoing education, both for refresher training and new-employee instruction.
- Conduct scheduled drills to bolster assignment performance; tabletop exercises should be included.

Communicate

Establish ways to immediately inform everyone in the organization when security issues emerge. Notify the outside world promptly and truthfully, but exercise extreme care in choosing what you say and how you say it. To the extent possible, your external communications should be planned in advance, perhaps with the advice of legal counsel to avoid potentially damaging public comments. Along the same lines, take pains to cut off damaging internal rumors regarding security incidents. Remember to include:

- Step-by-step procedures for alerting vendors, clients, partners, stakeholders, media, and, if appropriate, emergency services.
- Designate people to make these announcements to concerned parties.
- Staff specifically assigned and trained to answer incoming phone calls.
- Ongoing instruction regarding staff roles and responsibilities.
- A structured method of establishing what information can be shared internally and externally, and how serious issues should be stated.

Guard Against Cyberthreats & Other External Hazards

Bad actors distribute many types of malware, including ransomware, viruses, spyware, worms, adware, and others, all meant to inflict different kinds of damage to various parts of your IT operations. When cyberattacks, weather events or IT system failures occur, the challenge is to restore what has been lost and return to normal business functions as soon as possible. You need to assess what has been impacted, determine if the threat has been mitigated, and retrieve data via reliable backup solutions that are already in place. Using top-shelf disaster recovery tools will minimize your company's downtime and business disruptions.

Even with the best cybersecurity tools in place, catastrophes can happen at any time and can destroy a company in minutes. The only failsafe way to survive serious damage is to use an effective recovery solution. In some cases, this means the replication of your entire IT environment, including data, systems, hardware, and applications, at another location. Building a duplicate site is a daunting proposition, but good planning with expert guidance can minimize costs and simplify efforts.

Because security is so complex, there is a tendency to skip important steps. Although 3PL and trucking companies are always pressed for time, it is vital that you adhere to some essential priorities and best practices:

- Recognize that your company is responsible for its IT security; not the government, not professional associations, and not your security-solution vendors.
- To improve response and recovery, security and risk management leaders must align business continuity management with cybersecurity incident responses.
- Obtain cybersecurity insurance.

- Develop a data protection strategy to minimize the impact of a cyberattack.
- Erect the strongest possible firewalls.
- Eliminate RPD ports, which are vulnerable to external attacks, and instead employ VPN for RPD usage.
- Restrict access by outside parties to guest networks.
- Exercise your updated computer security incident response plans with an expanded response and recovery teams.
- Make a systems patch management plan. Be sure your operating system software, firewalls, and network routers are currently supported versions, and that you have installed all security updates (patches). For most sites, this means validation of your servers, databases, routers, network switches, etc., to meet the vendor recommendation patch levels. Security updates should be tested and installed weekly or monthly.
- Establish a crisis management team for the organization; the team will be responsible for managing all types of business disruptions.
- Create and maintain multiple redundant copies of all your important data.
- Make sure that your plans are thoroughly documented and regularly updated.
- Find ways to minimize downtime of critical applications and communications.
- Plan for a possible temporary shutdown of your physical plant and have arrangements in place for staff to work remotely.
- Exercise caution with data sharing; more than with most organizations, 3PL and trucking company management should know what data is being shared, where, why and with whom.
- Install high-quality backup and disaster recovery technology to ensure the preservation of data, systems, and applications.

Use Frameworks When Devising Security Methods.

They cut down on errors, foster teamwork, and ensure that plans are followed closely.

The National Institute of Standards & Technology (NIST) Framework is a set of best practices for organizations of any size or technical complexity. This Framework has three sections:

The Framework Core

- Identification
- Protection
- Detection
- Response
- Recovery

Framework Implementation Tiers show various approaches, from the most basic and direct (often the most effective for 3PL and trucking companies) to the most elaborate.

The Framework Profile squares plans with proven standards and practices.

The Center for Internet Security (CIS) Framework follows a well-respected crowdsourced model:

- Uses knowledge of and experience with cyber-attacks to shape cyber defenses.
- Steers security investments toward the highest threats.

continued on page 22

Specifically, the Democrats' framework outlines the following provisions:

- Brings existing infrastructure into a state of good repair and enables the completion of critical projects through long-term, sustainable funding.
- Sets a path toward zero carbon pollution from the transportation sector, creating jobs, protecting our natural resources, promoting environmental justice, and increasing resiliency to climate change.
- Ensures a transportation system that is green, affordable, reliable, efficient and provides access to jobs.
- Provides safe, clean, and affordable water and wastewater services.
- Prioritizes the safety of the traveling public.
- Helps combat climate change by creating good-paying jobs in clean energy, investing in energy efficiency and reducing greenhouse gas pollution.
- Expands broadband internet access and adoption for unserved and underserved rural, suburban, and urban communities.
- Modernizes 911 public safety networks.
- Creates family-wage jobs with Davis-Bacon Act and other strong worker protections.
- Supports U.S. industries, including steel and manufacturing, through strong Buy America protections.

One of the key pieces needed to move an infrastructure package before the expiration of the FAST Act in September 2020 is finding a long-term funding solution that shores up the Highway Trust Fund. The framework released by the House Democrats is essentially silent on how they propose to fund the $760 billion investment. The same is true for the Senate bill as well.

No matter how Congress decides to pay for the investment in the sustainability of our nation's infrastructure projects, the simple fact remains: our nation needs the investment now. Our crumbling infrastructure continues to fall further and further behind many other countries across the globe, and states cannot appropriately plan and budget for project investment without certainty from the federal government.

2020 will be an interesting year for sure on many different fronts in the political environment, but no matter if you are a Republican or Democrat, we need infrastructure investment now.

Chris Burroughs is Vice President of Government Affairs with TIA. He can be reached at burroughs@tianet.org.

SECURITY VULNERABILITIES ...
continued from page 13

- Recommends automating security protections.
- Collects members' best ideas.

Backup Your Data Thoroughly

Without effective backup, critical files can disappear forever, and the loss of information details can be damaging. Therefore, stored duplicate material should be absolutely complete, and for 3PL and trucking companies of any size, it should also be rapidly retrievable. In choosing backup solutions, keep these factors in mind:

- Speed of access to backup data.
- Automated capture and storage of data.
- Likelihood of the technology changing unexpectedly.
- Service-Level Agreements.
- Whether recovery speeds are specified or unspecified.
- Backup lifecycle management.
- Multiple versions of backup material.
- Backup material stored separately from IT systems.

As mentioned previously, it is best to replicate your IT environment at a safe separate site.

Develop a Disaster Recovery and/or Business Continuity Plan

When 3PL and trucking companies' business is interrupted, the ability to get back on track quickly is crucial. While good backup is a key element in disaster recovery, the two are not the same, and recovery methodologies especially must be tailored to the organization's needs. Every good disaster recovery plan should contain:

- Redundant copies of important data, systems and applications off-site.
- Tools and processes to recover copied material.
- Prompt restoration of communications.
- Fast restoration of the most important data and applications.
- Well-maintained and updated recovery processes with regular updates and evaluations.
- Ongoing training of staff in recovery processes and workaround methods.

Be sure to establish solid and thorough security procedures, along with the testing and auditing needed to maintain them. As your IT environment changes, you should test, audit and update your plan at least quarterly and any time your environment changes.

Now that security compliance has become a key segment of today's IT landscape, 3PL and trucking companies must embrace a full-on commitment to best practices if they are to prosper. For best results, that means the development of thoughtful and continually evaluated procedures tailored for your organization.

Chuck Cook, CBCP is President at Renovodata. For more information call toll-free at 877-834-3684, reference our website at www.renovodata.com, *or email us at* info@renovodata.com. *RenovoData is a leading, remote cloud backup and disaster recovery service provider, helping companies protect critical data worldwide.*