Cyber Threats Are Multiplying Rapidly

Protect Your Data with These Three Steps

By Chuck Cook, RenovoData

Cyber security threats are nothing new, but the recent explosive growth has become a global concern. News reports of such attacks have become commonplace. The September 20, 2017 issue of *PC Magazine* states that in the first half of 2017, there were 1.9 billion data items compromised worldwide, compared to 1.38 billion for the entire year of 2016.

While cyber-attacks against major corporations and governments make headlines, upwards of 70 percent of these breaches target small-to-medium businesses, including 3PL and trucking companies.

As the frequency of these incidents expands, governments around the world are working to stop them. However, the hackers never rest and their techniques grow ever more sophisticated. Fortunately, strong safeguards are available to defend against even the most aggressive and ingenious attacks.

Because assaults are becoming more sophisticated and more frequent, data security has become increasingly complex. To ensure effective protection, it is necessary to invest time and money in choosing the right tools, along with extra effort to fully utilize them.

The speed and constant activity typical of 3PL and trucking companies contribute to minor slip-ups that can have major consequences. Despite your efforts, the odds are not in your favor. One wrong click of a mouse from just one of your users can render your organization's data useless. From a data recovery perspective, where do you start?

Effective recovery from data breaches consists of three steps:

- The ability to recover
- Rapid recovery
- Planning and prevention

Ability to Recover

The ability to recover requires both ironclad file backup and strong disaster recovery capabilities. File backup and disaster recovery are not the same. Backup prevents data loss, but only disaster recovery can safeguard operating systems and other components that do not house data. Complete system protection must also cover infrastructure and auxiliary devices that are part of the emerging Internet of Things phenomenon. Because 3PLs and trucking companies have been quick to adopt such ancillary technologies, they should be wary of the potential risks.

In choosing disaster recovery solutions, it is essential that you carefully evaluate your specific needs. The products and consultancy you choose must accommodate every area of vulnerability. The constantly evolving nature of malware, with such new twists as RaaS (ransomware as a service) underscores the need to stay abreast of the latest cyber-weaponry.

> Organizations using encryption software and infrastructure are thought to be more successful in maintaining data security than those that do not.

Evaluating every element of your system has the additional benefit of identifying potential single points of failure that can easily be overlooked.

Organizations using encryption software and infrastructure are thought to be more successful in maintaining data security than those that do not. This may be because companies that enact thorough measures, such as universally applied encryption, are likely to take data security more seriously than others. When considering data security vendors, be sure that first-rate encryption is part of the package.

Rapid Recovery

Rapid recovery is necessary to fully benefit from your recovery capabilities. If your operations are stalled for any significant length of time, the steep and difficult-to-control costs of downtime will reduce productivity, damage employee morale, and hurt the company's reputation.

Rapid server recovery is a primary requirement. Without the right solution in place, it can take days or weeks to recover from a server loss, which can devastate any organization.

In evaluating data security vendors, look for one that can create an IT environment that comes as close as possible to uninterrupted operations. Every element of the system is replicated so that functional recovery can take place within seconds or minutes after an at-

Continued on page 14

Cyber Threats Are Multiplying Rapidly

Continued from page 12

tack. Such an environment should also strengthen backup and improve application uptime.

Planning and Prevention

Planning and prevention entails studying your company's specific needs, planning a course of action, and selecting the best available recovery tools and security performance packages. Build a plan that fits your business. Consider the must-have elements of your plan, including a business impact analysis, communication techniques, and the necessity of constant testing. Expert counsel is needed to keep your plan's development on a sure path.

Continually anticipate potential problems. What could go wrong? Will your vendors help? Who does what? Will your plans work? Who's writing this down?

Cloud storage, a key component of your security profile, provides availability and redundancy and also supports business continuity in the event of a disaster. Learn what to look for in choosing a cloud backup service. Companies housed where acts of nature or other catastrophic events could make the workplace unusable should look into setting up an alternative off-site location where IT functions could be moved intact and operations resumed quickly. This can be especially challenging for 3PL and trucking companies because of their complex workplace footprint.

Include your employees as partners in your planning and implementation. This includes non-IT user personnel as well as IT specialists. Seek their advice because when it comes to day-to-day operations, they are the hands-on experts.

Make it known that setting up security solutions will involve some interruptions and lost time. Both are normal and to be expected. Remind everyone of the benefits that strong security will bring.

Put together the best training programs you can, both during installation and periodically thereafter. Perform regular recovery drills to keep everyone up to speed. And be sure to involve your vendors in your education initiatives. They might have valuable resources and services which can assist you.

Finally, make certain that the vendors you choose understand the particular strengths and challenges of 3PL and trucking companies as well as being thoroughly knowledgeable about the current data security landscape.

The author, Chuck Cook, is President of RenovoData. Michele Vayle, Marketing Director, may be reached at mvayle@renovodata.com or (877) 834-3684.