Best Practices for Preventing Email Cyberthreats

PART III IN A THREE-PART SERIES FOCUSED ON CYBERSECURITY

Chuck Cook | RENOVODATA

JIRSAK/SHUTTERSTOCK.COM

TWO ARTICLES IN recent issues of *3PL Perspectives* outlined the challenges posed by email phishing attacks. The first described the most prevalent types of threats and the second explained how to identify them. This article illustrates the best practices for protecting 3PLs and trucking companies from those attacks.

In the second of the two previous articles, these defensive actions were recommended to guard against malicious emails:

- Check the salutation, the email address and the domain name.
- Beware of spelling and grammar errors.
- Take note of file formats and distribution groups.
- Verify that the sender can be reached and is legitimate.
- Never click on hyperlinks in questionable emails.
- Never divulge confidential information.
- Never respond to such phrases as "immediate action required," "account suspended," "unauthorized login attempt detected," or "your system has been compromised."
- Never click on attachments you don't know to be legitimate.

These guidelines are part of best practices, but the term also encompasses principles and activities ensuring that everything that should be done to guard against email phishing, as well as other types of attacks, is being done. Each organization's procedures and processes are different, and especially so with 3PLs and trucking companies. Accordingly, best practices vary from business to business. They consist of concrete actions that are clearly defined, thoroughly disseminated, and constantly reinforced and updated.

Company-Wide Acceptance

The entire organization must understand that mounting strong safeguards inevitably requires extra effort and time. This may be greeted with resentment and even push back on the part of some employees, so it is imperative that all staff buy into stringent adherence to defensive measures. For 3PL and trucking companies, the addition of new routine tasks can be in conflict with the speed required in conducting day-to-day business.

Designated Leadership

An early step in building a system of best practices is to appoint leaders to

devise, disseminate, train for, and oversee every aspect of the initiative. On an ongoing basis, these leaders should play a watchdog role in identifying the most damaging email scams. They should continually measure and analyze the results of the program and make updates and improvements as needed.

Training

Working with IT, management, and expert consultants, leaders should carefully plan and implement a training program. Instruction should be illustrated with examples of fraudulent messages, preferably with real phishing emails previously received by the company. It is also recommended that trainers be selected who have experience in presenting instruction. The best IT mind may or may not be the best teacher.

Strong Passwords

The best security in the world can be overturned by careless password handling. Strong passwords protect both the company and the individual.

- One key to a password's strength is its length. The longer the better.
- Incorporate numbers, capitals, and special characters. Going outside the alphabet makes passwords harder to break.
- Try substituting numbers and special characters for letters, such as substituting the number 3 for the letter e or the @ sign for the letter a.
- Consider a password generator. A number of these are available, and IT professionals and security specialists can help in choosing the best one. Be aware that because generated passwords are complex enough to frustrate hackers, they can also be hard to remember.
- Some passwords should never be used because they are much too easy to crack, such as "qwerty" or "1qaz" or "PASSWORD."
- Be sure to reset passwords regularly.

Tools

There are many products that can help reduce vulnerability to phishing attacks, performing such tasks as identifying and blocking poisoned emails; however, for smaller 3PLs and trucking companies their cost may be burdensome. Following best practices and planning wisely can provide safeguards without outside investment. Expert advice is available, so you need not face the email phishing challenge alone.

THE MEASURE OF BOTH A CYBER ATTACK'S EFFECTIVENESS AND A **VICTIM'S LEVEL OF DAMAGE** IS THE LENGTH OF TIME IT TAKES FOR THE COMPANY'S SYSTEMS TO RECOVER.

Prepare for Recovery

The measure of both a cyber attack's effectiveness and a victim's level of damage is the length of time it takes for the company's systems to recover. Effective disaster recovery from cyberattacks can be categorized in three maturity levels.

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

The Ability to Recover requires both solid backup and strong recovery capabilities. Bear in mind that backup and disaster recovery are not the same. Backup prevents data loss while disaster recovery protects operating systems and other components that may not house data.

Complete system protection covers an ever-widening range of infrastructure and devices. Proliferation is increased by the Internet of Things phenomenon. This is an especially important consideration for 3PL and trucking companies because they are quick to adopt new technologies and need to be mindful of the added risks.

Rapid Recovery solutions are crucial because no enterprise can tolerate extensive downtime. The damage to productivity, employee morale and company reputation increases as normal business activities are stalled.

Server recovery is a primary requirement for a successful disaster recovery program. If the right solution is not in place, it can be days or even weeks for servers to recover.

Planning and Prevention are the linchpins of a successful program. In planning for recovery, the most important metric is the real costs of each hour of downtime. Accurate calculations of these numbers will guide the entire planning process.

At the top of that process is the need to ensure that the organization's recovery objectives are in line with the implemented recovery solutions. You can assemble all the moving parts yourself, but a safe and thorough solution is available in the form of DRaaS (Disaster Recovery as a Service). In these pre-built environments, IT landscapes are created to closely mirror the actual systems, so that functional recovery can take place within seconds or minutes of attacks. The entire protective environment is covered, from data backup to full-scale disaster recovery. Besides cutting the risk of loss to a manageable level, DRaaS strengthens protective capabilities and increases productive uptime.

Trust the Experts

In-house IT staff and outside consultants can provide invaluable guidance regarding current technologies and proven techniques. Their knowledge can help hold down costs and lay the groundwork for future improvements and expansions.

Above All, Be Prepared

Email cyberthreats are constant, relentless and hackers are getting smarter. On any given day, an email phishing scheme could break through your defenses and cause harm. Although you may have some protections in place, they may not be enough. It only takes one crack in your armor for a cyberattack to break through, but with diligent effort and reasonable investment, you can maximize your email safety.

The author, Chuck Cook, is President of RenovoData. To learn more about cybersecurity, go to http://www.renovodata.com/blog/.