AVALON
RISK MANAGEMENT

Cyber Tip of the Week: Best Practices

October 23, 2015

More than ever, companies need to protect themselves against the threat of cyber security. The process is not as high-tech as you'd think, however. Below are some tips to ensure you are doing everything you can do on a day to day basis as well as an overall security plan.

User Education
This seems like a simple thing, but truly, user error is the largest hole in company cyber security. Be it phishing scams or emails infected with malware, if your employees don't understand how your systems can become infected, they won't know how to avoid the risks. This is needs to be consistent and constantly reinforced. New hires on-boarded should be given formal training on security systems as well as common sense cyber know-how such as no opening emails from unknown senders.

Systems Audits
Policies should be put into place to do routine systems checks on all networks and systems. Emails, servers, etc., need to be checked periodically to ensure things are working properly and that nothing has been infiltrated.

Manage User Privileges
Not everyone needs to be privy to everything. Create a system hierarchy where only people who require data can access it. It will also help network administrators track user paths more easily if something did go wrong.

Malware and Anti-Virus Software
Anti-virus system should be implemented throughout company systems and on all computers. A simple email can infect a whole company if not guarded against.

Removable Data Must be Monitored
This is something people don't often think about. That flash-drive you picked up on a tradeshow floor or was dropped outside of your building in a parking lot? They can contain malware that can lead to huge security breaches all because someone was curious about what was on an unknown drive. Reminding employees of this simple thing might be the difference between a normal day and interruption of business.

Control of Company Phones and Remote Access
Whether your employee is accessing your servers from home or mobile device, they could be exposing your system to security threats. First, software and firewalls need to be put into place to keep the bad things out. Security and networking companies can help you create system safeguards to assist with this. Second, and most important, is training. Everyone from the CEO to the hourly worker needs to be on the same page with data security. You can have the best cyber security system, but if people don't know how to utilize it effectively, it's useless.

The Quest Newsletter is designed to provide critical information in the transportation industry. Avalon Risk Management is not responsible for the