Truckinginfo
the web site of Heavy Duty Trucking magazine

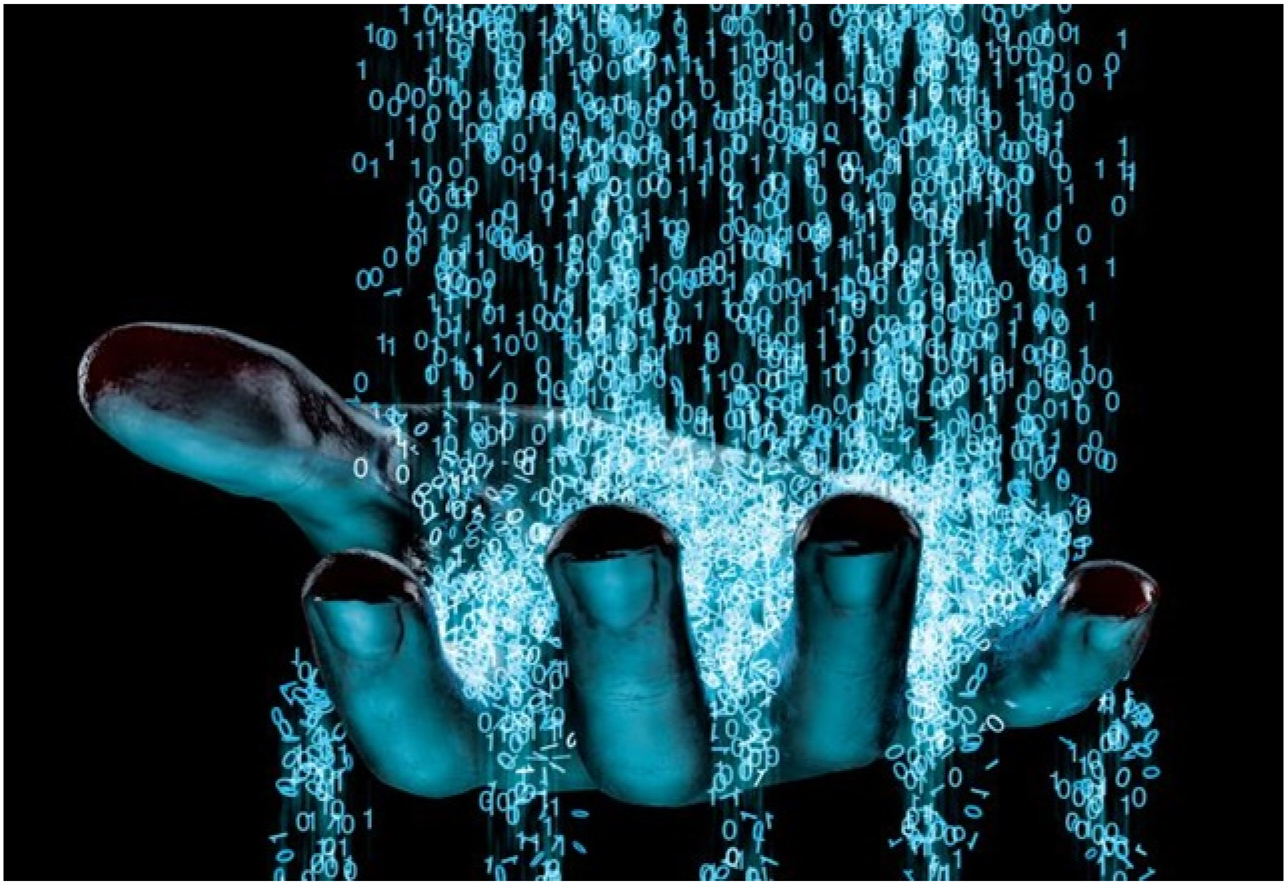
http://www.truckinginfo.com/article/print/story/2017/10/cyber-security-connect-at-your-own-risk.aspx

Cyber Security: Connect at Your Own Risk

IN PART TWO OF THE EIGHTH INSTALLMENT OF THE TRUCKING IN THE 21ST CENTURY SERIES, WE EXAMINE THE RISKS FOR TRUCKING COMPANIES IN AN INCREASINGLY CONNECTED INDUSTRY.

October 2017, TruckingInfo.com - Cover Story

By David Cullen



Connectivity — trucking shorthand for plugging into the Internet of Things — is a positive trend being advanced by industry suppliers and embraced by forward-leaning fleets to better control operating costs and boost productivity.

It all sounds good. Until it doesn't.

The appeal is easy enough to grasp. Connect every digital device so that data can be shared and leveraged across multiple, interconnected systems. In trucking, that means linking everything from in-cab computers to smartphones to hardware so reams of data can be intelligently managed and leveraged.

Expanding connectivity can make trucking operations smarter and nimbler and thus more profitable. But it also heightens exposure to cybersecurity threats. When everything is connected, a sophisticated criminal or merely a disgruntled ex-employee or unhappy customer can more easily gain access to computerized systems to wreak havoc on unsuspecting or poorly guarded businesses.

Ron Godine, vice president, information and cloud technology for fleet-management provider TMW Systems, points out that increased connectivity via in-cab devices gives outsiders the ability to “touch all the systems that affect the vehicle and learn your location. If they know your location, what can they do? How can they target you? There’s safety concerns with just knowing your location, where you’re going and how fast you’re going. Any of those things are a security awareness risk.”

Hackers can then gain access to a fleet’s trucking management solution and back office systems to learn about customers, loads, and financial information, cautions Godine. “What we’ve seen is that people can get into a system by automation and by hacking accounts, and then they peruse data like any other user.”

Alan Gordon, chief information officer of Cisive, parent of Driver iQ, which provides employee screening services, says that “small- and mid-sized companies can get lulled into thinking ‘Who would go after me?’ but truck fleets are just as much in the crosshairs as any business.”

Ignorance is not bliss

“The reality is that ignorance is bliss,” says Ben Wiesen, vice president of products and support for Carrier Logistics, which provides transportation-management solutions. “We would not go through life walking across eight-lane highways without looking. But we see numerous trucking operations doing just that when it comes to cybersecurity. The fact is wherever computer systems are operating, serious concern and caution should be taken” to avoid cyberattacks.

“As everything we use becomes more connected, the more risk there will be that criminals will gain control of computers,” he continues. “The IT industry dedicates huge resources to cybersecurity. On the other hand, fleets don’t think they’re in a tech industry. Yet fleets are so reliant on their computer systems. For all the nuts and bolts, the computer is the heartbeat of trucking.”

As for who is at risk for what, Wiesen says that typically depends on the size of the fleet. “Yes, there’s the risk of information being stolen on customers or drivers. But those are targeted actions with less likely reward when aimed at a smaller, lesser-known trucking company. It’s not a big risk for most fleets, but information could be stolen to poach drivers or customers.”

By contrast, he says, “the biggest risk is horizontal; that is, it runs across all businesses.”

Examples of horizontal risk include hacking or email planting to install malware, which can steal data or disrupt operations, and the newest threat — ransomware viruses. “Ransomware attacks are conducted by sophisticated criminal enterprises that effectively ‘kidnap’ a computer system remotely and demand a ransom to unlock it again. These attacks are a very real concern for everyone. They can take out any computer that has value to someone."

Ben Barnes, systems director for McLeod Software, reports that the fleet-management provider has helped nearly 30 customers that incurred ransomware attacks so far this year. "This type of threat has become huge to the average fleet." He says cyberattacks used to be aimed at specific businesses, like the massive breaches of everything from mega retailers to Hollywood studios, but "ransomware will attack any target of opportunity — it's a quantity approach."

Barnes says these crooks may only ask for $100 or $500 to release a machine from their clutches. Once the ransom is paid, however, "there's no guarantee they will give you the codes to release the computer. But if you have your system backed up or other means to recover your data, you may not want to pay at all. One company loaded up a new server to recover from the attack; others have paid because they did not have backups."

One high-profile transportation company affected by such an attack was FedEx subsidiary TNT Express, one of many companies hit by a cyber virus in June. The ransomware encrypted data on machines and demanded $300 ransoms for recovery. FedEx had to refer customers to its own network while TNT reverted to using manual systems to operate. At press time, it was expected that the company's quarterly profit would take a hit.

Wiesen also cautions that there is a potential for access through computer hardware on a truck (see previous story). "Think of the news stories about 'nanny cams' being taken over to gain control of a home computer. There has been concern expressed about hacking into infotainment systems on cars as well as what might happen with self-driving cars and all the connections they will have." And the same would go for commercial vehicles.

Whatever their chosen route of attack, Cisive's Gordon says there are two distinct types of hackers to deflect: the insider, and the external threat. The insider may hack into a program at any business for nefarious effect, while the external agent tends to target larger firms. "They know they exist — brand recognition — and will scan them for weak points where security protocols are not up to date. When they find a way in, they will exploit it."

He further distinguishes the enemy by what they are after. "Some hackers are disruptors who say they do it because they love a challenge, while others are bona fide criminals. They will go after credit card data or customer lists and sell those on the 'dark web.' And there's also corporate espionage that goes on. Hacking to get ahold of internal information on customers and pricing, sometimes sold as 'competitive intelligence.' And there is ransomware, which is a growing threat."

Gordon sees the main external vulnerability for fleets as having outdated or unsecured operating systems. But he says that's easy to fix, as "most use software that continues to receive regular security updates," adding that third-party software run on your systems must be secure, too. He also cautions that a lot of fleets have customized software. "Especially if this is web-facing, it must be written with an eye to security. Also, a lot of firewalls are only concerned with what is going in. But you should also watch outgoing data to help counter any insider threats."

Wall off the threat

TMW's Godine says the aim of cybersecurity is to "put more walls" between criminals and your valuable data. These include using encryption and multi-factor authentication, which beefs up the traditional username/password by adding such authentication factors as PIN numbers, trusted device authentication, and fingerprint, face, and even voice recognition.

"It's about making the wall high enough or making multiple walls that hackers have to climb over. You can't just put in one solution and be done. You have to put in multiple solutions, because any one of them can be compromised."

On the other hand, cyber criminals and other bad actors might just sneak in through holes in the walls — especially if you make it easy for them. That is to say, "clicking on that email" remains the most common way to launch a security breach.

That's why it's just as key to drill staff on adhering to security protocols as it is to invest in high-tech security measures. Godine advises fleets to make sure they have a digital access policy — and that it's enforced and reviewed. "Usernames and account passwords should have appropriate complexity. Default passwords, easy-to-guess passwords, similar passwords used across the company should all be avoided. People go 'ho-hum' at that stuff, but that's the way most people hack into systems."

Lloyd Palum doesn't see fleets being any more likely than other businesses to incur cyberattacks. The chief technology officer for Vnomics, which provides fleet-management solutions, says the difference is that truck fleets may be unaware of the threat. For example, someone could hack in and disrupt dispatching.

Palum says the best line of defense for fleets, as for any business, is to stay on top of threat assessments and commit to following best practices for cybersecurity, including securing communications and keeping software up to date in a timely fashion. "Bear in mind that in many attacks, wireless and Wi-Fi systems are targeted, so you want to keep those as secure as possible. Regularly updating software is critical to avoid falling prey to known risks uncovered since the last updates were issued. Fleets are typically not well-versed in cyber best practices, but [technology] vendors can advise them."

The best defense is a good offense, he says. "You always want to confirm that all the 'actors' on your network or systems are always behaving as would be expected." Actively monitor for "anomalous actions" that could signify a cyber breach has occurred or is being attempted. He notes that there are service providers that can be contracted to monitor network behavior.

Palum also suggests that fleets without full-blown IT teams may take comfort from computing in the cloud. "Cloud computing is nothing more than renting space in someone else's computer," he points out. "If you're using a reputable cloud provider, they will be on top of cybersecurity. They actively monitor their networks.

But you do need to know that data coming to and from those computers to yours is secure and that all system users are authenticated."

McLeod's Barnes recommends wielding "a tool bag of stuff" to help prevent cyberattacks. "Your defense has to be company-specific, based for example on how open your systems are to the internet," he says. "There are preventive best practices to put in place, such as educating users on security protocols, and putting a recovery plan in place as you would for any other contingency that can shut down your business. You want always to be in a preventive role, not in recovery mode."

Related: Protecting Your Data