The Internet of Things Introduces Big Possibilities for 3PLs and Trucking Companies…Along with New Security Challenges

By Chuck Cook, RenovoData

The Internet of Things (IoT) has been with us for a while, starting with Internet applications for cars, phones and other personal devices. As IoT applications multiply, they are revolutionizing the IT landscape. Founded on widespread wireless availability, IoT applications consist of several components: sensors, which gather and transmit specific types of data using application software and middleware, and the cloud, which supports communication between devices.

Most of today's sensors simply gather and transmit basic data, but upcoming generations will perform more extensive IoT tasks, leveraging gathered data in increasingly sophisticated ways. The IoT will help us create new technical ecosystems in which we will drive smarter cars, work in smarter environments, and live in smarter houses, neighborhoods and cities.

Just about every enterprise will be impacted. For example, factories will become exponentially more productive and efficient, and highway systems will become faster-moving, safer and cheaper. Undoubtedly, 3PL and trucking companies will be among the most broadly involved in and affected by this growing technology, both because of the proliferation of internal applications as well as IoT products used by related organizations.

As with all breakthroughs, new problems have already arisen, with more on the horizon. On both personal and business levels, issues of privacy and confidentiality have already taken center stage. More ominous still are data security risks. What is different is that the more potential entry points a network contains, the greater the possibility of penetration by malware. By definition, the IoT will increase those points. This kind of risk will be of special concern to 3PL and trucking companies because of the fast pace of their environments and the number of tasks that will be enhanced by the IoT.

In addition, some developers give security short shrift in their rush to get new products to market as quickly and cheaply as possible. These developers are under no legal obligation to build good security into their offerings.

But no matter what the IoT has in store, data security basics have not changed.

For all its promising possibilities, the IoT is no more nor less than an expansion of the Internet. Although the number of IoT applications is growing, the principles of solid network protection are the same as ever. Again, what is different is that the IoT expands the potential entry points for malware attacks. To stay ahead of the expanding opportunities that hackers are finding with the IoT, we offer these recommendations.

- Reinforce your security program, and let your customers know that you intend to meet IoT-related risks head on.

- Bring trusted vendors into your IoT security planning program early in the process.

- As with other security threats, take special care to protect your email, and stay informed about how to make web browsing safe for your employees.

- Because data security will become even more complex than before, you can expect the expansion of your data protection to require extra study and effort.

- Review your server recovery capabilities.

- Stay abreast of current trends in malware.

- IoT applications are cloud-driven, so as they become integrated into your IT profile, be sure to reevaluate your cloud-backup resources.

- You are likely to need new kinds of tools to deal with threats posed by the IoT. When the time comes to acquire those tools, choose them wisely.

- As these threats emerge and your defenses are strengthened, keep your employees in the loop. Make them full partners in your security program.

The IoT will bring exciting new functionalities to 3PL and trucking companies, and we should all stay informed about the latest innovations. But no added capabilities are worth increasing the risk of a data breach, so proceed with caution.

Because the IoT presents new and unique risks, your vendors, current and future, must fully understand the specific IoT vulnerabilities faced by 3PL and trucking companies. These vendors must be armed with the techniques and tools needed to meet your every data security challenge, including those of the IoT.

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