Katzscan Newsletter

July 2014

katzscan®

Supply Chain Operations & Technologies
Supply Chain Vendor Compliance
Fraud Detection & Reduction
Good Governance
Turnaround Help

Since January 1996

The Internet of Things (IoT) is essentially the connection of all things across the Internet. It is the communication of sensors on the food package as it is consumed or close to its expiration date communicating to the sensors in the refrigerator or on the dry shelf to alert the consumer and send data to the consumer's local grocer who will automatically shop, package, and deliver the groceries to the consumer through the grocer's own or a third-party delivery service, and the knowledge of where the delivery vehicle is moment by moment. It is the continual monitoring for condition exceptions of medical devices on patients as they move through their daily lives. It is sensors in supply chains and on manufacturing lines driving more data for analytics of machine performance and quality control. It is the knowledge of where in-transit goods are and at what temperature during their journey.

According to the article titled *The Internet of Things Is Here. What's The Most Vulnerable?* in the February 2014 issue of CIO magazine, all this connectivity may come with a cause for concern. The article lists five vulnerability areas where hackers can gain access – and even control – resulting in not just theft of data but in some cases trigger disaster.

[1] **In-vehicle Wi-Fi** – hackers can gain access to the smartphone data that connect to the vehicle's Wi-Fi system; I will add that **V2V** (vehicle-to-vehicle) technology hacking of driverless vehicles is a scary proposition indeed! In-vehicle sensors already involve radar-reliant braking, blind-spot warning, and lane detection.
[2] **Mobile medical devices** – hackers can gain access to mobile medical devices, possibly taking control and causing death, as well as spoofing the data they are sending back to the medical facilities; even accessing mobile sports fitness products can yield private information about a person's health that may be compromising or sensitive to the to the person's employer or family
[3] **Wearable Devices** – hackers can infiltrate wearable devices such as Google Glass® to glean the information they are recording and use that information for nefarious purposes as information is collected personally and professionally
[4] **Retail Inventory Monitoring** – hackers could intercept the real-time inventory data being sent to a retailer's systems and falsify the information, forcing a retailer into making purchases and stocking inventory it does not need or, conversely, under-buying and running out of stock when it should have been making buys
[5] **Private-sector drones** – according to the article insurgents in Iraq intercepted a U.S. Predator drone because its signals were not secure, and at the invitation of the Department of Homeland Security a Texas A&M University student infiltrated one of the university's drones with incorrect GPS information and sent it crashing to the ground; as drones become more prevalent they become the sources of an attack

Without necessary security protocols installed, I am just not sure that all this connectivity is completely trustworthy. As a fraud-fighter the door is wide open for illicit behavior to infiltrate and infect enterprise information systems, resulting in incorrect decisions. And as more decisions are automated through the supply chain the ripple effect is likely to be costly. It is risky enough today to attach a personal computer to the Internet without a good firewall and anti-virus software; the thought of livelihoods and lives hanging in the balance of all these unsecured sensors is more than just a little unnerving. I think that along with real-time auditing or check-and-balance programs, supply chain systems can be made more trustworthy, but some of the other vulnerability scenarios make me wonder if the world is secure enough for what lies ahead or if we are rushing naively into even more trouble than we have today.

Thanks.

Norman Katz, CFE, CFS, CCS, MOS
Katzscan Inc.

Look for the book --> http://www.gowerpublishing.com/isbn/9781409407324

0 95494 24141 1

Visit our web sites:

http://www.katzscan.com/

http://www.supplychainfraud.com/

http://www.vendorcompliance.info/

http://www.turnaroundhelp.com/

http://www.supplychainsox.com/

Do you know of a company - *maybe your own* - suffering from disconnected dots?

www.disconnecteddots.com

Let's link!

www.linkedin.com/in/katzscan

Follow Katzscan on Twitter!

http://twitter.com/katzscan

Katzscan is on Facebook!

http://www.facebook.com/katzscan

The opinions expressed herein are not intended as any type of financial or legal advice.

Click to view this email in a browser