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

Since January 1996

Security concerns of Internet-connected interconnected devices

In the series reboot of *Battlestar Galactica*, Commander Adama, played by actor Edward James Olmas, strictly forbid the networking of the Galactica's primary computer systems together for fear that doing so would allow them to be compromised by their machine-enemy, the Cylons. He was proven correct in several episodes as to how keeping critical systems such as navigation and defense segregated and disconnected was a winning move against a cyber enemy.

In July 2015 Jeep was forced to recall 1.4 million vehicles after it was discovered that hackers could infiltrate the computer system of various vehicles and take control of the automobile's navigational control mechanisms, e.g. braking, acceleration, and steering. The hackers gained entry via the vehicle's entertainment system and then made their way to the automobile's connected control systems.

Fiat-Chrysler labeled the hacking a "criminal action." However this does nothing to wipe away the fact that 1.4 million of its vehicles – and possibly more – were vulnerable. Criminal – by who? The automaker or the hacker?

According to a Bloomberg News article in the July 31, 2015 Miami Herald, drug pumps can be hacked resulting in too much or too little medicine being delivered to the patient, in either cause causing life-threatening injury or death. The United States Food and Drug Administration (FDA) has issued a warning to healthcare providers that drug pumps called Symbiq manufactured by Hospira should be taken out of use immediately because they can be hacked via the healthcare facility's wireless networks.

And as reported in the September 4, 2015 Miami Herald, certain baby monitors do not have basic security features which make them vulnerable to cyber-hacking. The results being that unknown persons may be watching your little ones, and that the unsecured baby monitors could be used to take control over other WiFi enabled devices in your home such as a security system or a personal computer. Security lapses in the baby monitors included unchangeable and hidden passwords or a lack of encryption of their data streams.

With the figurative explosion of Internet-connected devices, one must consider security before connecting these devices and relying on them, especially when it comes to life-altering consequences. Sensors may not be that smart, only capable of registering simple environmental changes, but the interpretation of those changes is why device security needs to be implemented at the connection source and within the device itself. This is no different than protecting a computer with a firewall and anti-virus software.

We also have to think of the practicality of some devices being advertised as Internet-connected: just because you can does not mean you should. What will an Internet-connected thermostat provide you that a traditional thermostat does not? Do you really need a mobile banking application to check your account balance every hour? Is it necessary to have household appliances connected to the Internet? Are we really comfortable with devices around our house that record what we say when we talk to them, and are they really not listening when we tell them not to? Ask yourself if the feature is a must-have or superficial add-on the next time you consider a product purchase. How much more of your personal identity are you willing to shed and lose control over to an inanimate product that is the face of one or any number of consumer product or – eventually – marketing data companies?

Ultimately as consumers we have the power to control what we purchase and what features companies include or exclude in the products we buy. We need to ensure our products are safe and reliable, and this needs to include hardened against hack attacks in the upcoming age of the Internet Of Things.

Thank you.

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

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

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