Katzscan Newsletter

January 2017

katzscan®

Enterprise Resource Planning / Electronic Data Interchange
Supply Chain Vendor Compliance
Fraud Detection & Reduction
Revitalized Operations
Information Insights

Since January 1996

Security in the age of the Internet of Things

The holiday season is behind us and with the start of a new year everyone is just beginning to enjoy their new gadgets, from baby monitors to video doorbells to interconnected thermostats and other household appliances. But before you get too comfortable, you might want to keep reading as I refer to the October 2016 Reality Check editorial in Business Solutions magazine (www.bsminfo.com).

There are an increasing number of cybersecurity threats being hatched and launched on a daily basis. Webroot, a threat and security software and services company, informs that 6,000 new phishing sources, 80,000 new computer malware applications, and 51,000 new mobile malware applications are discovered by the company every day. Yahoo, used more by the older and less technology savvy folks, is the primary site to be spoofed for phishing, and Wells Fargo has overtaken PayPal as the most spoofed financial site. According to Brian Fonseca, director of the Jack D. Gordon Institute for Public Policy at Florida International University's Steven J. Green School of International and Public Affairs, the global cost of cyber-attacks is anticipated to grow from the current $400 billion today to a projected $2.1 trillion by 2020.

Ransomware is a growing problem, but the payments are increasing as criminals are no longer satisfied with ransoms of just a few hundred dollars. Different data has different value, e.g. healthcare data has a higher street value than other data.

Gartner estimated that 6.5 billion "things" could be connected to the Internet in 2016, and that number could jump to between 20 and 34 billion by 2020 depending on whose estimates you choose to believe. That is a whole lotta things.

And to mass market those things, some manufacturers have been a little lapse on the security side. Previous stories of how easy it was to hack baby monitors have been around for a while. But consider what a hacker could do with control of a thermostat or other household device: instead of requesting just a monetary ransom while keeping the environment the device is managing stable, the criminal could alter the environment having taken over the device.

Imagine having your home's thermostat set to 98 degrees or your refrigerator and freezer being set to high temperatures, spoiling your food until the ransom is paid. What is your recourse to ensure the criminal does not repeat the offense after the ransom is paid: to change out the unsecure appliances? Will the appliance warranties cover these security breaches?

I am very happy with my programmable thermostat and disconnected appliances that are off the grid, seeing no reason whatsoever to be so connected to my house that I need to know what my appliances are up to in my absence. While this might make for a funny animated movie, there is nothing funny about a criminal hijacking a home and doing untold disrupting damage until a ransom is paid, perhaps over and over again.

Happy New Year.

Norman Katz, CFE, CFS, CCS
Katzscan Inc.
954-942-4141
http://www.katzscan.com

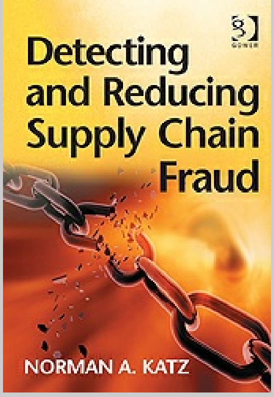
0 95494 24141 1

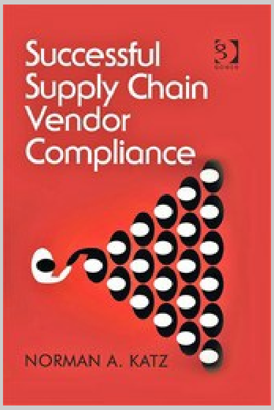
Interested in either of my two books?

Contact me for an author discount code before ordering from my publisher.

Both book titles make for engaging conference and event speaking topics.

Contact me to speak at your next conference or event.





Both books are the first titles on record on *their respective topics!*

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

Copyright (c) Katzscan Inc.