HIDDEN SENSORS

Jack Davidson

Shortly after I changed my snow tires, the tire pressure warning light came on. Assuming that I had a malfunctioning sensor or a bad seal, I headed back to the shop only to discover that my spare tire, after years of inattention, had slowly lost enough pressure to trigger the warning light. I had wasted several hours simply because it never dawned on me that my spare tire had joined the growing list of wireless devices that now inhabit my world and needed to be checked. A world that is becoming not only more complicated, but immediate. A world of sensors designed to help me if only I could understand them.

So I started tabulating wireless devices: sensors in my tires, phones and TV remotes, wrist watches, table alarms (set by satellite), wireless speakers, garage door openers, lights, and a neighbor who remotely starts his car to avoid triggering his wireless motion detector. The list keeps growing.

Then it dawned on me. Do I understand the risk of wireless?

After reading "Being Digital" in 1995, I concluded that the author, Nicholas Negroponte, predicted a future that I did not think would have a significant impact in my lifetime. He painted a picture of walking into a room and having buried sensors in the curtains immediately alter the room temperature to adjust to body temperature. Negroponte's prescience is well known in technology circles. He predicted that touch-screen technology and voice recognition software would become the interfaces of choice. The phenomenal growth of iPhones and iPads suggest that he was on the mark. And the mark, in Negroponte's view, is a bit and not an atom. He writes about atoms, which make up physical, tangible objects such as CDs, books and letters, and he believes that in the future all forms of information that are now made of atoms (books, CDs, etc.) will eventually be turned into bits.

He visualized the Kindle in its embryonic stage. My book-lined study, the newspaper waiting to be picked up on the porch, the CD's   and records, they are all history. It is sad, and it is inevitable. Surrender is our only alternative. If, as you read this, your inner voice says, "I will never give up hard copy," my bet is that within two years you will be owning a Kindle.

I was not prepared for the future. Nor are many Information Technology (IT) Departments.

One of my responsibilities in the company is to protect data. When data is streamed through wires, it is easier to control. Now, some of the data floats through the air. Are we ready?

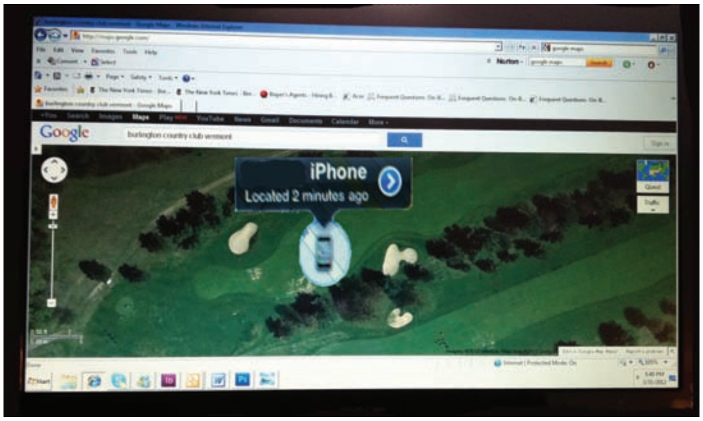
Certainly, our staff is aware of the dangers of using unsecured networks. Some free networks were set up by hackers with the intent of stealing your data. Other wireless networks, like those in schools, coffee shops, restaurants, and hotels, are also often unsecured and vulnerable to hackers, who can use inexpensive programs that serve no other purpose than to steal your data.

Wireless
(Digital Information Floating through the Air)

After studying the iPad for about six months, I concluded that it would very helpful to us in a number of ways, some obvious and some that might be classified as "intuitive." I thought I had sufficient business reasons, but only on-the-job utilization would reveal the true extent of the value to us and our clients. I also concluded that every employee should have an iPad.

For an employee-owned company, a decision of this magnitude would ordinarily require a deliberative process. Uncharacteristically, both the decision and the deployment were very rapid – so rapid that I actually lost an iPad whose whereabouts continue to remain a mystery.

Consequently, I immediately installed software that will find a lost iPad. In the process, I inadvertently found another sensor. I used a test subject in our Burlington office and tracked an iPad from my laptop to 286 College Street, where one would expect it to be. But in so doing, I discovered that the software also tracked the person's iPhone, which I found about a mile away. I zoomed in, selected a satellite view, and discovered that the iPhone was on the sixth hole of the Burlington Country Club, and in motion! That hurt; client golf, and I didn't get invited!



Tablet purchases dominated the holiday sales, and the most popular one was the iPad. Growth in the use of these devices is extraordinary in all sectors of our world. In a business environment, it is very important that those using a tablet or smart phone understand that they are now in the world of the wireless. In a wired world, we can trace wires and for the most part protect the data that passes through them. In the wireless world, we need to be very careful.

Not only is the iPad designed for transferring data wirelessly (via either 3G or wi-fi) , it is designed to store the data externally. Its slim case can hold a healthy amount of data but probably not enough to keep both you and Apple happy. Apple, for starters, wants to sell you music, books, movies and software programs. Over time, I am sure they will develop miniature hard drives large enough to hold all the data hidden in the slim iPad case. But their sales opportunities will be greatly enhanced if they can get you to store your data on their servers. Ipads are designed for Clouds.

The Cloud

There are many definitions of Cloud Computing. My definition is a picture. Imagine a wireless connection to one very big server in the sky that stores your data. Clouds are provided by many organizations, and they can be dangerous. They are frequently designed for data mining. They are marketing sensors on a grand scale. They are also targets for hackers. Companies that do not control iPad and iPhone use are discovering holes in their security networks. In the old days, the IT department bought and controlled the company devices. Now, the employees bring in their Christmas gifts – the iPads, iPhone, Droids, etc. – and start storing company data in the Cloud without the intervention of the IT Departments. Historically, IT Departments were often viewed as obstacles to innovation, and some, if not many, companies still need to change their cultures in this regard.

"It was much nicer before people started storing all their personal information in the cloud."

Fortunately, in our company, our auditor is very involved in the process. She is both creative and risk-averse. Innovators here don't feel a need to bypass her, and I worry less about data security.

How to Reduce Cloud Risks

Recently, one of our investment managers received a heartfelt e-mail from a client whose message said she was stranded in Scotland after her purse was stolen. She wanted us to send money by Western Union to their office in Glasgow. We responded with two questions: what was your mother's maiden name, and where was your father born? The response was interesting. The father, who had been born in San Diego, was in the opinion of the responder born in Liverpool. When we responded, noting the failure to furnish the right answers to both questions, the return response was, "Well, I was very tired last night when I received your e-mail." Our client's e-mail account had been hijacked! Whether you use a public cloud, such as Google's Gmail or I-Cloud, or a private cloud that we use for some storage, your first concern is to prevent hijacking. The best way to do this is with your password: the longer, the better. Using length, even more than complexity, is the best way to ward off computers that can generate thousands of passwords in mere seconds. The best password combines both length and complexity, but herein lies a problem. If you have to change your password often, you may start to sacrifice both.

The Nobel Prize-winning physicist Richard Feynman fooled his co-workers into thinking he was an extraordinary code-cracker. They were unaware that he simply walked around the office at night and found their combinations on calendars and scraps of paper.

There are different schools of thought on requiring periodic password changes. The IT Department's reflex is to tell our clients to change incomprehensible 15-digit passwords often. Yet studies have shown that users will simply create easy-to-remember passwords. We have decided to lengthen the change cycle to five years for our clients who access their statements. Our clients now can decide which school of thought to embrace, and they can choose to change their passwords more often. Our staff, on the other hand, have to use a newfangled fob that is fed codes every minute from a satellite and change a combination of 3 different passwords frequently in order to gain access to similar account detail.

It is also important that we do not use the same password for different important sites. Using the same password twice for important data is hazardous.

So yet again, protection becomes more difficult: complex, lengthy passwords proliferate, and they are all different!

The answer may be a password manager program which allows us to enter highly complex passwords that we will not have to remember so long as we can remember the one password necessary to get into the password manager program. We are now testing Roboform. (Even if its Cloud were hacked, that wouldn't reveal all your passwords, since the program works by storing part of the encoding information in the Cloud and part on your device.)

Syncing to the Cloud

If your desktop, tablet and smartphone can sync, you may be able to gain access to the same information on the road, at home, and work. If you have a need to synchronize your data, you probably have three options:

1) You can sync solely to the Cloud. Unfortunately, you create a risk that the information will be unavailable if you do not have internet access or if the Cloud is ever hacked.

2) You can also use the Cloud to store information in two or more locations so that if you do not have access to the information on the internet, you will be able to retrieve it from your laptop or desktop. In addition, multiple storage locations will provide backup if your hard drive malfunctions or your Cloud gets hacked. Unfortunately, information on the Cloud may be vulnerable. James Fallows, in the November 19th issue of Atlantic Monthly last year, discussed the aftermath when his wife's Gmail account was hijacked and all of her correspondence, photos, and other records for a six-year period simply vanished. She had stored everything on Google without a copy on her hard drive.

3) Use the Cloud as a drop-off station where you transfer data to each device and then remove it from the Cloud. Although more secure, this option is not particularly user-friendly.

Conclusion

As much as I love my iPhone and my iPad, I also mourn the loss of the hard-cover book and the depth of stereo phonograph records, which dwarf the quality of flat digital re-recordings. Furthermore, I now have to stay continually vigilant regarding security.

Perhaps one day we will coax the data genie back inside the safety of wires and cables. Some of us are waiting for the "Negroponte Switch." Prescient Nicholas Negroponte predicted some time ago that digital information that is currently going through the ground (i.e, in wires and cables) will eventually pass through the air, which is where we are today. He also predicted that the data would soon return to the ground after new high-speed broadband cables alter our lives yet again.

I would like to take comfort in the "Switch" but, unfortunately, my imagination again fails me. I cannot imagine my colleague tethering her device on the golf course.