A View From the Prairie

Vol. XXIV No. 10 October 2017

Internet of (Vulnerable) Things

In Nature documentaries, we can watch penguin colonies raise their chicks. We can watch the adults come and go with food and finally the chicks make their first splash in the ocean. All the while, right off shore, the sharks are swimming, waiting for a meal, knowing that the adults and chicks will swim right into range. The concentration of penguins means that the shark is very likely to get a meal.

Currently, there is a mad rush into the Internet of Things. Yes, the opportunities are huge. The benefits will be large to industry when every piece of equipment can report on its health. There is some extra convenience when consumer devices can be controlled from a distance. But the spread of unsafe devices is putting all of us at risk.

With the Internet of Things, the "sharks" are "swimming right off shore" here too. The problem is that almost none of the consumer level devices being built can be guaranteed to be safe now or even in a few years. The recent discovery of a major flaw in the WiFi encryption protocol shows the problem. Every WiFi device: phone, camera, front door lock, washing machine, heart monitor, or industrial machine needs to be updated to fix this flaw.

But in many cases, we do not have a way to update the equipment. Medical equipment and inexpensive home devices often have no way to be updated. Or worse yet, have "back doors" for such updating which can also be exploited by the "sharks".

Yes, the "sharks" are out there looking for these things. The Mirai botnet is but the first example. Millions of "Internet of Thing" devices were compromised to be used for a destructive attack on several web sites. Others have been compromised to mine bitcoins.

Most people do not worry about their use of such insecure devices. In many cases, the problems come not from one compromised device, but in the power of many compromised devices. When millions of devices can be controlled by one bad actor, the whole network can be put at risk.

Foreign Actors Can Use Them Against Us

This risk is not just because of criminals or unhappy young men wanting to shut someone up. The risk is that national enemies will take advantage of these capabilities to perform cyber warfare against us. Already, the Russians have been testing other methods such as GPS spoofing (which is giving our Navy and Air Force real problems). What could North Korea do with this? Iran and Saudi Arabia have already engaged in multiple cyber-attacks on each other.

We are at risk. Our purchases of cheap "Internet of Things" devices may easily become a national vulnerability.

As we spread Internet of Thing devices into our power grid (for the very good reason of better control), we may also spread the very way for an enemy to bring our power gird down on command from their office.

We will need to figure out how to detect and isolate such vulnerable devices.

Ignore Stuff

The human body is receiving a huge amount of data every second, most of which we ignore. Our eyes are processing every second and send the data to the brain on a network of about a million nerve cells. We toss away most of this information.

In management, often we need to ignore certain things. With any group of people, there are those who will "push the envelope" a bit. . Many of these cases can be safely ignored but there are some that should not be.

The cases that we need to not ignore are those that violate our basic principles. These can be cases where laws were violated, people harmed, or our ethics crossed. We do need to know if such a case is a rare event or is a chronic issue with a person. Even small problems that are chronic issues are ones that we need to address as they will cause problems with customers and with other employees.

It can be easy to try to set a new policy every time we find a problem. However, it is far better to keep the list of policies small and enforce the important ones. We only have so much time and energy with which to enforce policies. When we have too many policies to enforce, the wrong ones generally get enforced and the important ones are overlooked.

There are managers who try to "spy" on their employees. In many cases, this happens when the manager does not understand what is being done, does not know how to tell if any progress is being made, or how to tell the quality of the results. In today's information economy, it is far better to focus on learning how to measure the results than to worry about how many hours an employee is working, where they work, or which hours they choose to work.

A View from the Prairie is published by Prairie Trail Software, Inc.,

Making *Information* from Streams of Data

1-800-618-4199

www.prairietrail.com

Risky World

With the Internet of Things so vulnerable to being hacked, there are a couple of attempts to forcibly clean up the situation. A couple of hacking programs are designed to turn the vulnerable device into trash. These programs hack into a device and feed it a set of commands that erase memory and turn off internet access.

Prairie Trail Software, Inc

3821 Beaumont Lane
Plano, TX 75023

Address Service Requested

Prairie Trail Software, Inc.

Making *Information* from Streams of Data

We offer

Custom Software Solutions

To Business Problems

Generating More Profit

By Automating Processes,

Simplifying Communications,

And Reducing Errors

We pull the whole system together
- or just the parts you need

Business Process Automation

Database Design and Management

Cloud Services and Applications

Web Services and Servers

Custom solutions to meet your needs

Call 1800-618-4199
www.prairietrail.com