A View From the Prairie

Vol. XXVI No. 6

June 2019

Computer Security is Everyone's Responsibility

Computers are everywhere and on everyone. Some people are carrying multiple computers at once. No longer are computers huge boxes living in sealed rooms. The result is that computer security is everyone's business. There are some important principles for security. These are: A security breach can destroy a company. Security is both a technology and human practice. Security is a moving target and we need to build resilient organizations that can survive.

A security breach can destroy a company. No matter what size of company you have, a security breach can destroy the company. Most security breaches are where data gets out to our harm. Loss of the bank account, or customer data, or leakage of new product or process information can be very damaging. There are now new laws that make loss of customer data even more damaging.

The other major security breach are the computer viruses such as "ransomware" which encrypts your hard drive and demands a ransom to get the key to unencrypt it. These may take down one computer or the whole network. While many companies have paid the ransom, there is no guarantee that the key will be delivered or that some other party hasn't also encrypted your hard drive. There are reports of multiple ransomware on a single machine. In many cases, it is far better to scrap that machine and start over from the backup.

Security is both a technology practice and a human practice. No matter how good of a technology one might use in a safe, it doesn't help if the combination to the safe is posted right next to the safe door. People need training in security matters and why security is so important. Top management needs to know about the risks to the company from computer security and the need to invest in security practices.

Security is a moving target. We want to be able to buy a safe and rely on it but we can't. Whenever there is enough value, people figure out ways to break into such safes and new ways to rob information. Recent reports of how researchers have figured out what they call "side channels" to get into some smart phones really show how many different ways people can get at information. (One case is where the researchers started simply with sending bad WIFI packets to the device and that gave them a backdoor into the phone.)

To make our organizations resilient in the face of such problems, we need to rethink the value we get from being connected and new ways to protect that value. Having current (and tested) backups and using encryption on all important data is the starting point. Some companies practice attacks including sending "phishing" attacks to staff to see who needs further training. Other organizations are actually going back to typewriters and paper "because nobody can hack a typewriter."

We need to keep aware of computer security issues and be willing to redesign our computer systems if they put the company at risk when they fail or are hacked.

Resiliency In the Face of Data Breach

Market Irrationality and Want to Believe

The market is known for being irrational. Fads come and go. Companies that are losing money badly go for a public offering and get priced as if they were making huge amounts of money. We offer a badly needed service and people don't buy it. Markets are irrational and can stay irrational far longer than our wallets can survive. We want to believe the irrational stories.

Such irrationality is based on our human "want to believe". We want to believe the company CEO when she promises a fast and cheap way to test for many human diseases. We want to believe the person offering us a chance to make money without working so hard. We want to believe the television preacher who promises that if you send him money, money will come your way. We want to believe the business person who claims that he can run a far larger enterprise even when he has no experience in that area.

Market irrationality and the "want to believe" is deep within our human DNA. We learn from stories far more than from "dry data". People build whole organizations on anecdotes. Having multiple stories sells a lot of books, but the stories may be incomplete or mislead.

And then, we do not know how to handle when our beliefs are wrong. Often, when our beliefs are proven to be wrong, it causes such deep problems that we do not have the capacity to change those beliefs. That is why there are still people who believe the Nazi or Stalin era propaganda. There are those who have given all to a ministry believing that it would take care of them only to face poverty.

We do better when we face and accept reality no matter how difficult it may be.

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

Making *Information* from Streams of Data

1-972-618-4199

www.prairietrail.com

Risky World

In places where people are being mugged for their smart phones, a thriving business of fake phones is happening. People buy the fake phones to hand to the muggers. The phones power up and show the same startup screen, but don't do anything else.

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

Fractional Time CIO

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 Intelligence Dashboards

Database Design and Management

Cloud Services and Applications

Web Services and Servers

Custom solutions to meet your needs

Call 972-618-4199
www.prairietrail.com