

30th Annual FISSEA Conference

March 14, 2017 to March 15, 2017

Author: Sherry Dinkins, BS Information Computer Science, 1987

Address:

Midwest City, OK

Email:

Cell:

To: Mr. Clarence Williams, NIST

Mr. Williams,

I received an email regarding this conference and found the request for proposal and the Contest. I am not seeking to participate in either activity.

I found the topics very interesting and thought that I would share a few words. I looked for a format but didn't find one outline. So, I will just use a conversational style.

Summary

The topics listed on your main page for the conference all seem to have one common root. How to stop the unrelenting attack on our systems? There is a common thread that runs through the failures. Accesses to the systems are no longer restricted by physical controls.

All of the training given to the public and employees and yet the systems remain under a constant state of failure. There are two forces that seem to drive this unusual trend. It is the multigenerational workforce and the need for a "at home feel" in the workplace.

At this point in IT history, the focus needs to go back to recovery. The door to Pandora's Box is open and the Baby Boomers are dying out so there is no one to close the lid. They are being replaced and all the knowledge of the "lids" is walking out the door.

Opinion

My career has span almost 40 years. I started in IT when the degree program didn't exist. I went to Andrews University in Berrien Springs, Michigan. The degree required 191 credits. I had to learn how to write code, setup a business and mathematics. If I had decided to stay another quarter, I could have had two(2) degrees, BS in Information and Computer Science and a Minor in Math.

When I was leaving Border Patrol and going to California Department of Transportation, I called Andrews and spoke to the Head of IT Department. I asked the director why my degree was not in the catalog. He laughs and said, it was too hard and they had to redesigned the program. When I graduated in 1987, I think it was only about four or five of us that completed the degree program.

I started my career towards IT in the early 80 when Word Processors were all the rage, I have watch the industry go from a straight Ethernet backbone to routers and VLANS, WANS and all the other various configuration.

My first job in 1988 was with the Superconducting Super Collider in Berkeley, CA before we migrated to Dallas, TX. I can remember building Netware 1.0 servers and other systems that are in museums today. You would get the hardware in one box and the Red Box from Novell in another box.

You had to know what you were doing to just get it to work.

But things began to change, windows servers won because they were easy to setup, NOT secure, but easy. The new kids on the block didn't want the problems of a Novell server that could operate with errors, broke drives and smoking hardware.

Then you had the need not to go to people's desk to resolve problems we could remote in to their desktop. Then, this was added to servers so that they could be checked from outside the network.

Remove the restrictions on the ports to make it easy on the WAN team so they didn't have to open the port to the outside per correct authorization.

Then servers became blade boxes no monitors, remote access from the outside.

Then you had the evolution of all the project management products. It is interesting to me that they used the SDLC as a way to do an IT project. Yet, they didn't read the Mythical Man Month, by Frederick Brooks. The development of software requires a person to take an idea and create a reality.

Designing a network system requires taking a physical product and constructing it so it meets the requirements of an idea. These are not the same.

They want the structure but not the constraints and “got ya’s” for a lack of a better term. I have seen people manipulate the numbers in MS Project and other programs to hide the slippage in a project. The approach today has become so confusing the actual timelines are all hidden.

Then the backups went to a cloud that was a virtual storage without defined drives. If the cloud failed, you lost everything. It is hard to back up a cloud. This idea was to save money on hardware.

Then the certification started, if you had the money you could get the certificate but the person with the skill would be asked to train them.

The new kids wanted the same toys that you have at home. I was always told, “it works like this at home”. The stuff at home had no security and was constantly changing and failing. I watched the cell phone industry create a “storm” of epic proportions.

I have a Blackberry still. I got into a heated discussion with a rep in a cell phone store about four (4) years ago about the lack of security on the android systems. They wanted to give people little mini computers with no security of any kind. We can see the impact of that decision on people’s lives from the fraud and phone data breaches.

The “home work” idea took off in the work place. The Blackberry was dropped and the “fun” phones were embraced with joy because they had all the cute apps that they use at home.

These and other changes have created a “home work” look. Everything is loose and feels easy to use. The box is open; there are no defined lines between fun and work.

I had to look all over the place just to find a printer that didn’t have WiFi. The current configurations have created the perfect storm that we are seeing. If you look at the various operating systems, it is configured with numerous rules that allow “remote” access on all kinds of levels. It doesn’t ask you, it just loads when you boot the system.

I am currently developing some seminars on ID Theft, Scams, Credit Report and Repair, etc. I am offering them to the public for free. I purchased a notebook with USB connection, a portable projector. When I was checking out the notebook, I was shock at the rules that allow remote access. I mean it was about 90%.

This is your perfect storm. Hackers can go from device to device. All of the systems I designed and built had a disaster recovery component. It is not if you will fail, it is just when. I wrote a paper at University that correlated the chance of a business surviving depending on how long it took to recover from a data center failure.

The longer they are down the life of the business diminished. I was accepted by PMI to work towards a Project Management in DR. I bought all the books and read all the material. I called my rep at PMI and told him that all of the material contradicted or was filled with conjecture. I said the position puts all the blame on the Project Manager for the failure. You had to be person who could read the future. I

expressed my concern that it was the Project Manager who was responsible for getting the various factions too corporate. The course work was inundated with those required skills.

I never took the test. One job could run your career. Set your training not for money but for skills. You cannot teach a person to be a true System Analyst. It is a skill that is a gift or is nurtured by working with someone who has the gift.

If you walk into a large data center and the floor falls out, what do you do? Is anyone there able to take some of the tangled equipment and build a system or do you need to call the manufacture? We have gotten away for knowing how to take junk and make a system in an emergency.

What about all the legacy system that are ageing out? The people that built them are being replaced. Like me, I am in the IT group that has the highest rate of age discrimination, 66, according to Congress.

I retired from the California Department of Transportation. I built the Disaster Recovery solutions that were mandated by the Legislators of California. When I retired in 2011, because the new kids didn't want to maintain it, it was replaced.

The storm is here. I have two (2) Videos in my presentation on Scams. One, is title Defend Against Ransomware _ Federal Trade Commission, he basically states the only defense is having a backup that will get the company or person back. Two, is Cybersecurity 101, PBS.ORG/Nova/labs, he basically states we know the internet has problems and is not secure but we have to work with it to make it better but not so good we cannot have fun.

Conclusion

People are so accustomed to having a "home work" it is not going to go back. Your best training will be in teaching people how to get back. The baby boomers don't understand "home work" that is why the people are still clicking on links like they do at home. The system allows the executable to run and connect to the network through one of the remote rules.

The Storm is here.

Sir, I have enjoyed the work that NIST has done over the years and the work you continue to do with such excellence. Thanks for sharing your time with me.

Sincerely,

Sherry Dinkins