Cyber Security

…what you should be concerned about…

by Kat Rowoldt

Things we never think about, don't want to think about, but need to think about -- would be a quick synopsis of the Cyber Security in the Trump Administration Conference I attended in San Antonio. It was presented by St. Mary's University Center for Terrorism Law.

The timing of the conference could not have been better. This was about one week after the cyberattack in Europe which shut down countless businesses, affecting 100's of thousands of people, including hospitals, because the hackers took their victims' computer systems hostage for ransom. This, in reality is a daily occurrence. We seldom hear about this type of terror attacks.

I remember a year ago visiting a computer business and talking with the owner of the company about some things I was developing. Our conversation was interrupted when he got a reply to his request for the ransom needed to unlock the computers for a business he services. That was my first awareness of this issue. He discussed buying bit coins in order to pay the ransom, then hoped they would unlock the computers once the money was paid, and the stress of the company which was virtually out of business while this situation was being worked. Cyber warfare. It's here. It's happening. It's concerning.

Two weeks ago, I was blessed to video the conference. Dr. Jeffrey Addicott had saved a special seat on the front row for me so I could capture the whole conference for those who were not able to attend. It would be impossible for me to even begin to share with you the depth of information this conference contained in a basic article, but let this whet your appetite to listen to some of the presentations.

I found myself seated in a conference room filled with some of the best computer minds in the nation, from military to major international players in cyber security technologies. Some of these people must make in an hour what I hope to earn in a year. It was a most interesting mix of people who had come together to hear one another share the latest things they are developing, discussions on issues they are dealing with, and stopping just short of publicly discussing what they are creating for what they see coming down the pike. There were several moments when the whole discussion was way above my understanding.

When talking about cyber security, there are a variety of angles and approaches that must be addressed. This was what I found fascinating. It wasn't just cyber hacks invading the guts of your business through the computer system, but it was security concerns from insiders, blackmailing of employees, etc. What all entails cyber security was so much larger than I ever imagined.

Colonel Michael Cote, Director of Communications, 25th Air Force, talked of a heightened threat level beginning in 2011. It sounded like he was involved in locating Osama Bin Laden through his cyber security work. He referred to his work as being watchers of the watchers. He was an interesting speaker.

Jeff Barnett, CEO, BESL, former military, has spent the last eleven years developing a very specialized area of cyber security. He deals with risk management for corporations. He discussed the dangers of those closest to us. In the rush and busyness of our days, things can easily happen because someone simply wasn't thinking, lacks higher ethical standards, or is simply untrained to recognize the various ways a cyberattack could be approaching your business.

We are familiar with phishing emails. Today they are getting harder and harder to detect because of the quality of their appearance and approach. Employees need to be trained to alert everyone immediately if they detect or suspect phishing emails coming into your business. Speakers constantly reminded us not to click on links in emails. That's the magic key which opens all kinds of horrors.

Cyber terrorist attacks, like the one that just happened in Europe which even made our news, target businesses, hospitals, and other key industries to lock up their computers so no one can get online to do their work, retrieve records, etc. They are held for ransom and generally are unlocked once the ransom is paid. Typically, the ransom can be as low as only $50.00, but the time lost, information at risk, and other threats can be devastating to a business. Hospitals cannot retrieve medical records for the patients in their care. Scary.

One suggestion which was made by a panelist was to have more than one server with your information on it. Never have all your information on just one server. If you are attacked and locked up, having a shadow system in place, will keep you from being completely shut down while you are dealing with the attack. You simply pull your data from the other server to continue working.

Surprisingly, it was reported that eighty percent of all cyber incidents had insider assistance either through their lack of knowledge or because they had an actual plant in the company. This is an amazing fact and shows our "trusting" society mindset is putting us all at risk.

These are the key points the speakers shared with us:

- Limit admin access
- Keep your financial records on a different server
- Reduce your attack surface
- Upgrade security every six months
- TRUST NO ONE

Watch for things like spoof emails. They can look like they are from the CEO of the company making a more compelling cause to click on a link, send back critical information, or more.

Train your employees. Change them from being problematic insiders to security detectors.

This was interesting. Criminals will cause you to erase all data, removing their evidence on your computer. When your computer starts acting weird, typically you call IT and they come in and hit the reset button (laymen's terms) which restores the computer back to its original format, removing all evidence of the criminal activity that had been happening through your computer with or without your knowledge.

Had you ever considered microchips in your pets could be controlled by someone? How about the fact someone could take over your pace maker? An incident occurred in another country where someone hacked into a hotel and sealed/locked all the guest rooms. No one could enter or exit. Whoa!

Two other key things that caught my attention were thumb drives and family members. Major corporations are concerned about people bringing in a simple thumb drive they could insert into a computer in a matter of seconds which could infect data or be used to lift information. The other grave concern is family members of employees being used by terrorists, as hostages, to cause key employees to breach security for their benefit. These are things we don't think about. Yet these are things corporations are dealing with today.

Consider the amount of data about yourself that is stored in computers all over the country/world. Medical records, insurance, banking records, Facebook, various social media platforms, school records, and the list goes on. Consider what would happen if someone manipulated or changed your medical records, created new data on you in a social media format, or simply erased your existence. What if gas pumps were cyber attacked and locked where they could not pump gas or simply drained your card accounts? The nightmare is real.

The growing industry for tomorrow is cyber security. There is a tremendous need already in this field. Encourage your kids and grandkids to consider this

path for their future specialty. With our dependence on computers and technology, this is tomorrow's mega industry.

Here's the agenda from that day so you can select which videos might be of particular interest to you.

Welcome – Dr. Stephen Sheppard, Dean of St Mary's School of Law
Charles E Cantu, Distinguished Professor of Law

Cyber Security in 2017 – Daniel W Southerland, Associate General Counsel
U. S. Department of Homeland Security

Insider Threats – Panel Discussion
Jeff Barnett, CEO, BESL
Colonel Michael Cote, Director of Communications, 25th Air Force

Navigating the Sea of Cyber Security Threats – Panel Discussion
Moderator: Martin T. Tully, Akerman LLP
Keith Lowry, Nuix
Jason Straight, UnitedLex

Achieving Cyber Compliance & Risk Management – Panel Discussion
Moderator: Martin T. Tully, Akerman LLP
Jason Straight, UnitedLex
Keith Lowry, Nuix

Lunch Address by Fred Burton, STRATFOR

Responding to a Data Breach – Panel Discussion
Moderator: Martin T. Tully, Akerman LLP
Joel Heft, Equifax
Keith Lowry, Nuix
Jason Straight, UnitedLex
Herbert Joe, USPTO

Key Note Address – Chairman, Michael T. McCaul
House Committee on Homeland Security

Cyber Security Challenges – JD McGraw, CEO, Ironclad Encryption

Closing Discussion – Dr. Jeffrey Addicott, Director, Center for Terrorism Law
Professor of Law, St. Mary's University School of Law

Until next time…

Kat Rowoldt

Christian Reporter News
www.ChristianReporterNews.com

If you enjoyed, please forward to a friend and share!