2018 Legislative Ag Chairs Summit
January 5-7
Kansas City, MO

Breakout IIA – Cyber Security

Moderator Dana Brooks from Land O' Lakes, introduced the speakers, Geoffrey F. Jenista, Cyber Security Advisor for Homeland Security and Justin Kosar, Cyber Compliance and Security Specialist at the Associated Electric Cooperative in Springfield, MO.

Before the discussion began, Ms. Brooks passed on some helpful information she had received from her company's cyber security advisor was 'Know who your local cyber security FBI experts are in advance, and then know the steps, should you need them, so you're not scrambling once you have a problem.' You should put a plan of action together for business and home or government for what you do in case of attack.

Recent IT Attacks

Geoff Jenista started off. The No. 1 Hack last year was the Federal Reserve. They were after everyone's email address and passwords. Everybody averages about 19 websites, most of which all use the same Username and Password. If the hackers can get one, they have compromised your information. The next four most important hacks were medical records.

The year prior was all the financials, but banks and financial companies have gotten good at shutting down a credit card in under 20 minutes. But if they can get your username and password, then they can start coming after you. The biggest threat to your organization is inside staff. If they click on the wrong thing, they potentially let these threat actors in. Educating your staff is critically important. The Target hack was done through the HVAC company that supported that building. The entire agricultural industry is tied through computers.

Background clearance, as in the military, listed all relatives and neighbors. If they break into this data, they now have all this information. It's all electronic. China's big hacking focus is intellectual secrets – patents, proprietary information – and sell it back to the U.S. at a cheaper price.

There was a hack of the NSA – they downloaded all the tools that government is using. There are viruses that are designed to effect so many people across the internet they shuts down the U.S. web in under twenty minutes. Now these people on the dark web have all the NSA tools, and they're coming after businesses and people.

The Costs

Average cost of a malware attack to a corporation is $2.4 million. Every person's information you lose costs $300 for that person. Equifax was every adult in America. It cost Equifax $750 million to protect their individuals. It takes 50 days to recover from it. Amazon makes $10,000 a minute. If they're down for 9 days, that's a lot of minutes. Bitcoin only charges $50-50,000 on whether you're an individual or company is because the company's reputation is worth more than $50,000. They'd rather pay that than get it in the press. An individual would rather pay $50 to get your home computer back. You pay it and don't notify the police. If they hit 100 million people times $50, it adds up fast, and it's untraceable.

Who Is At Risk?

Every person who has a computer, if you only have a singular account that has administrative privileges on it. If you click on the wrong thing, that virus suddenly has administrative rights to your computer. The easiest thing to do is to build a second account that just logs in with the click of a mouse, and secure that administrator account.

When you work for a corporation, they limit the rights of their employees to download and navigate. This is why they do that. It prevents you from accidently installing bad things, which then hop laterally throughout the

network. Businesses pay $50,000 to hackers. The average business that gets hit by a cyber-attack is out of business in under two years, because of reputation.

Smart refrigerators and security, etc. All of these connect to the internet. Show Dan, a site that finds IP addresses and publishes them. So if they can get into your refrigerator, they can get into your home network. Utility companies, etc., is a window for these people to get into your computer. Home Depot was attacked by a man sitting in the parking lot, because they were running a wireless network from the cash registers back to the servers. Anything wireless is susceptible to hacking.

Top Five Threats and Weaknesses

- Socially engineered malware (through Facebook, Twitter, and others).
- Password fishing attempts.
- Unpatched software.
- Social media blackmail
- Advanced persistent threat (slow password attempts)

Help is Available

Homeland Security has very helpful offerings. Contact them for assistance. They do assessments and management leadership. Resources are needed for IT security. Legislators need to advocate for this funding. There are 10 FEMA regions, with people all over the U.S.

HOW CRITICAL INFRASTRUCTURE IS BEING PROTECTED NOW

Justin Kosar was next to speak. He gave his background, which dealt with infrastructure modernization in electrical utilities. In addition he worked on designing, maintaining and securing the architecture of the systems. He then took a position dealt entirely with cybersecurity.

The control systems of the power plants have traditionally been Air Gap. There is no network connectivity, no wireless connectivity into these systems from the outside. Traditionally there hasn't been a huge focus on cyber security with these systems. However, now there are more threats from things like Stuxnet, where a plant that is air gapped still gets infected by malware. The industry is starting to take these threats much more seriously.

Ways to Protect Systems

Associated is part of the Cooperative system in Missouri and parts of Iowa and Oklahoma. They are a three-tiered system, and he works for the generation component. Below that are transmission components, and below that are distribution cooperatives.

The protections are on protecting the generating assets, and the command and control center that control the grid. Those are the key assets they're looking to protect. There are government regulations on how they protect that. NERC – the North American Electric Reliability Corporation – who writes a set of standards called CIP – the Critical Infrastructure Protection.

They oversee 800 regional organizations that work them the utility to make sure that they're following the rules and have strong protections in place. These vary from identifying what assets are the most important in the system, to giving guidance on how to design networks (setting up physical security perimeters, and electronic security perimeters) Monitoring the systems, the rules on how they're configured, what software can be installed, what communications are allowed to all of them. There's over 120 different requirements on what the technical controls are for all of these power systems.

The Recovery and Response Plans are some of the most important things that they have. There is no way to be perfect all the time, and so knowing what to do when you have a problem is critical. They not only have a

plan, but they practice the plan through exercises where they can simulate an emergency and go over the things to be done for recovery.

Recently they have begun doing Penetration Tests. They hired a firm of 'ethical hackers' to come in and attempt to penetrate the system. The company sits next to them and have tools to monitor what's going on. The hackers tell the employees what they are doing and the company will try to figure out how to stop them. These exercises allow them to tune their monitoring resources to stop the attacks as soon as possible. Most of the time it's not some magical code the hackers inject into the systems. It's always a person making a mistake somewhere.

Fishing and Solutions

One of the most common mistakes is fishing. The hackers in one instance spoofed an NRECA Website and lured employees to click on a link and give information. They are very sophisticated. The hackers learn about the company and learn how they can actually trick the employees.

They are a cooperative, so they need to protect the electrical grid as a whole, not just their own company. So they cooperate by sharing their IT department and offer them training and services.

They are members of the Cyber Mutual Assistance Program. They work under Non-Disclosure Agreements and work to help each other for emergency recovery.

The three things you can do to protect yourselves:

- Fishing – Something you can do for your company is to send out fishing emails to employees – fake emails that you can monitor and track.
- Passwords – quality of passwords is critical. If you have to write down passwords, do it only if you do not reuse them. Reusing passwords is broadcasting them to the dark web. Also, use long passwords of random characters, and use a password manager, too.
- WiFi - which is not safe

The Field is Growing

There are layers of security. Defense in Depth is a term for the various layers of security that exist. Detection, users getting better at finding threats. It takes more people and resources to increase the detection. His company needs more people trained in cyber security, especially industrial experience.