Smart Connections Conference

Scenario #1 - The company that handles your IT just went out of business with no advanced warning. No one is answering any emails an the phone number for the business says it has been disconnected. Your internet just went down and no one can access their documents or files.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
3	1. You will need to get a new company in. 2. There are two different issues - internet access and data. 3. Do we have access to our backups? 4. Do we have a disaster plan to refer to?	1. Don't know anything regarding contract. 2. Don't know whether the county has footprint documentation. 3. Don't know who would take the lead.	1. Everything in #3 if not available; make sure disaster plan is in place and we have a "what to do". 2. Make sure you know where your backups are and that they can be used manually or electronically. 3. Audit contractor to be sure the terms of the contract are being handled before something happens.	1. Get to know your neighbors. 2. Work with other counties and IT resources. 3. Do not think it can't happen to you.
1	1. Call Joel Rohnert 2. Contact another neighboring county that does have an IT department. They may know a somewhat local option. 3. Hopefully someone has a book of administrative passwords. 4. Check if there's an old contact from that company that maybe would be willing to moonlight.	1. Whether or not we had our own passwords.	1. In the future make sure that all admin passwords are stored locally. 2. Hire an IT person, if financially possible. 3. If hiring an IT person is not an option, then make sure to hire a more reputable IT firm to manage your network. If possible contact other counties to see who they suggest if they use an outside company.	1. Make sure you have a record of all of your admin passwords on site and readily available. 2. Do your research on the people that are managing your ID equipment in managing your network. Make sure that they are reputable to mitigate the chance of them going out of business and leaving you without support. 3. Hire someone if possible that can be on staff.
2	1. Contact ISAC \ ICIT for a vendor. 2. Get equipment on the way or internet provider en route. 3. ICIT emergency team en route.	1. Password, IP, vendor, contacts. 2. Is network equipment up, server up?	1. Documentation and disaster recovery plan. 2. Backup vendor 28e with other county.	1. Backup internet provider and service agreements with additional vendors

Scenario #2 - A public health nurse lost her laptop over the weekend. It was in her car, but now it is not there. She has not spoken to the police.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
4	1. Report to police. 2. Report HIPAA Security Officer. 3. Notify County Attorney. 4. Check with IT to determine if device is locked, able to be located and able to be wiped. 4. Was it accessed? 5. Inventory of what was on device.	1. Was it a personal or work laptop? 2. Was it stolen or lost? 3. Exactly when was it taken?	1. Add encryption to laptops. 2. Ensure secure password and dual authentication. 3. Update policy procedure for laptop use and storage.	1. Develop and follow policy and procedure.
5	Be Proactive: Install Bitlocker on all mobile devices Step 1: Call IT Step 2: IT disable all accounts connected to that laptop Step 3: Call police, file report Step 4: Remote wipe/locate if Apple device Step 5: Document issue, make sure it is tracked. Step 6: Issue new device to user	1. Username 2. Applications user had access to serial device number.	1. Installing Bitlocker on all mobile devices. 2. Have written policy for situations of lost or stolen devices. 3. Inventory.	1. Treat device like your own and make sure employees are responsible with devices they are allowed to take home.
6	1. If it was encypted no big deal. 2. If I was not encypted or encryption status was unknown, then we have problems!	1. Was it encrypted? 2. What data was on it? 3. How many people would be affected if data was lost?	1. Training - don't leave laptop in car! 2. Encrypt all mobile devices!	1. Call Joel Rohne, he'll take the fall!

Scenario #3 - The FBI calls the auditor and informs him that all of the county employee records with personal information have been posted to a hacker site.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
8	1. Validation of identity of reporter and if a breach actually 2. If a breach took place to what extent and what information was breached or leaked. 3. Identify possible sources of that information to begin to locate the origin of thay breach. 4. Locate the source and terminate any existing connections and make employee notifications. 5. Begin damage mitigation.	1. Is this a legitimate notification? 2. If in fact it is, did come through correct operational channels. This could be a phishing or other attempt to gain illegitimate access. 3. Also what personal information and who? 4. If this is legitimate, how was the FBI notified? 5. Who else was notified and when?	1. Depending of legitimacy - if illegitimate claim, who is calling and what are they attempting to access? 2. Why? 3. What system was breached and how? 4. Are proper systems in place to protect this data? 5. Were they functioning properly, updated and patched? 6. Was it caused by software/hardware/ an employee/former employee/vendor? 7. Was security in place for those possible vectors? 8. Emphasis on training, if the cause was by human error or implementation of better practices if software/hardware.	1. Share the experience, what happened and what it took to identify and correct. 2. What steps were taken in detail to mitigate damages and steps taken to prevent it from happening again.
9	1. Determine if it truly was the FBI by contacting IT or vendor. 2. Assume its legitimate, until determined otherwise. 3. Contact BOS, County Attorney, law enforcement and follow incident command protocol. 4. Depending on outcome contact employees.	1. What is protocol? 2. Need report from intrusion software or vendor.	1. Better understanding of importance of IT. 2. Refresh training. 3. Devote more resources to protecting and updating systems. 4. Review user permissions. 5. Are we collecting more info than we need on employees? 6. Tighten computer use policy/whitelisting.	1. Have protocol in place to handle such event. 2. Have meetings on how to protect and report such indicences. 3. Update software and tier patches.
7	1. Verify that the person calling is real. 2. Contact Sheriff, IT, and County Attorney. 3. Get Department heads together	1. If the threat was real, FBI information and credentials.	1. Have a plan	1. Share details of how it happened, so they would not become victims.

Scenario #4 - The treasurer clicks on a link to update the county's bank account password in an email he received which opens the bank's homepage. He logs into the account and changes the password as directed. The next day he gets a call from the bank stating that the $275,000 transfer he made the night before put his balance below the county's minimum threshold.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
11	1. Put hold on bank account. 2. Unplug or shutdown pc. 3. Contact IT Department. 4. Call FBI. 5. Scan pc. 6. Cry	1. Where money went to.	1. Need training on phishing emails.	1. Tell other counties about what happened so they are aware. 2. Also check with bank if get email about changing anything with bank accounts.
10	1. Contact the bank and halt all transactions. 2. Contact Sheriff's offices and start investigation. 3. Save all emails and browser history on computer. 4. Reconcile account for other transactions besides the $275k.	1. Other transactions. 2. Transferred to and from account numbers.	1. Email security education. 2. Additional authentication layers to access the bank account (verbal confirmation on some transactions).	1. Email security education. 2. Additional authentication layers to access the bank account (verbal confirmation on some transactions).

Scenario #5 - An employee from the recorder's office can't open any documents on her computer or the shared drive. She has a message that popped up on her desktop that says her files have been encrypted, and she will need to pay a ransom in bitcoins to get her files back. It's soon discovered that every server has all of its files encrypted as well.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
13	1. Isolate the initial system (if known), remove all internet access, create test environment to test backups, if backups are usable, restore from backup. 2. Notify banks, other partners and law enforcement.	1. What was the initial point of infection? 2. What type of ransomware - what are all of the demands/instructions? 3. Types of backup (disk, tape, offsite) and accessibility to backups? 4. Types of files that are encrypted?	1. Educate users on how to respond to a scenario if this were to happen (who to notify, what to do with their system - disconnect from network by unplugging the network cable and turning off wireless.) 2. User prevention training and training on how to disconnect from the network.	1. Provide user training and do simulations, if possible. 2. Scheduled testing of backups and restores. 3. Patching of all systems. 4. Use of necessary methods to help prevent user error (antivirus, firewall, etc.).
15	1. Contact IT Vendor or IT Employee 2. Restore from backup	1. How long will it take to restore? 2. Are our backups good?	1. Education. 2. Have a public response policy in place. 3. Compartmentalize county user accounts.	1. Have a plan in place. 2. Test your backups. 3. Don't think it can't happen to you! 4. Stay up-to-date on patches.
14	1. Contact IT. 2. Ask IT if they have a backups. 3. Notify an outside party (ie FBI). 4. Have IT conduct an assessment and disconnect primary internet connection.	1. Who to contact outside of the organization. 2. Formalized plan for response.	1. Have an incident response plan. 2. Fund IT properly. 3. Mandatory education.	1. Fund IT properly. 2. Encourage education.

Scenario #6 - The BBI and DCI show up at the Courthouse on Monday morning with search warrants to seize your servers because of criminal activity in your systems.

Table Number	What was your response to this scenario?	What information was needed that you did not know?	What changes are needed in your county in response to this scenario?	What advice would you give other counties in response to this scenario?
17	1. Contact IT. 2. Verify credentials of agents. 3. Call County Attorney or Sheriff to verify warrant. 4. Deply DR Plan.	1. If you can, deploy DR Plan. 2. Do they have a BAA for HIPPA?	1. Review DR Plan with employees.	1. Make sure you know your IT environment. 2. Know the procedures.
16	1. Check credentials. 2. Contact IT, Sheriff, County Attorney, Board of Supervisors and department heads. 2. Reformat the drive.	1. Physically seize the servers or they can do it on site. 2. The nature of criminal activities. 3. Do they need to take the server?	1. Policy 2. Training 3. Table-top exercises (simulations)	1. Hire the right people (avoid inside job). 2. Create policies. 2. Have training. 3. Engage in table-top exercises (simulations).
18	1. Call the county attorney and sheriff.	1. What is the scope of the search? 2. Can't take all servers. We would offer to clone specific servers but due to critical operations can't shut down entire network.	1. How do you plan for something like that? 2. Evacuate the public and lock the courthouse to the public until things can be discussed. 3. Have a contingency plan in place.	1. Have a plan and add this scenario to your contingency plan.