Anatomy of a Data Breach

Lessons Learned

- Recommend Cyber Security Insurance
    - The "coach" is invaluable in getting your through the entire process (computer forensics, guidance to your leadership team, knowledge of required notifications, the notification process itself (letters, call center), and credit monitoring/identity theft coverage.
        - The "coach" runs the show. His/her experience in the laws/notifications is important to keep you on track with your investigation.
    - Contact the person who does all other insurance for the District. This is something that is added to existing insurance plan.
    - This is a process that will take some time to complete, so get started now.
- Have your Computer Security Incident Response Plan (CIRP) in place.
    - Important to identifying when you need to notify.
    - Defines technical team
    - Defines leadership team (Superintendent, Academic Officer, Safety & Security, CFO, Risk Management, Public Affairs)
    - Auditors are now asking to see your policy/procedures and plan for responding to data breaches.
- If a breach occurs, document everything. Keep a running log of events. Things get really confusing and a good log of events will help you respond to other needs throughout the data breach process.
- If you've been breached, get FDLE involved at the beginning
    - They will want your system for computer forensics, but make sure you get an image of the device from them. Your Computer Security Liability staff will want to do computer forensics immediately. FDLE cannot guarantee a quick turn around on computer forensics.
- If your data is breached by a third party, it is still your data and you are still ultimately responsible for your data. You will want to control the communications with your customers and not leave that to the third party.
    - Everyone is guilty until proven innocent.
    - The finger pointing (between you and your third party vendor) can start early. Stick to the facts that you can prove, don't make assumptions.
- Log files:
    - Log files become very important in determining what occurred and when. Do you have log files? How long do you keep them? This breach went back two years. Do you review them? We know this is an almost impossible task because of the sheer volume of logs. Recommend you use security as a service to help you manage your security environment. They can analyze your logs.

- SFTP/FTP:
    - Where are your credentials stored? In an Excel file on your network? Consider an enterprise password management program like LastPass.
    - Is your vendor using SFTP versus FTP. If not, consider not doing business with that vendor.
    - Are you sending an encrypted file to the vendor? If not, talk to your vendor about implementing that feature. This protects your information even if the third party FTP site/network is breached. Especially if the vendor leaves your files in the FTP region for any length of time.
    - Minimize the amount of data you send. Do the vendors really need all the fields they are requesting? Remember it is not just the SSN you are worried about it is privacy information as well.
    - How many FTP sites are you running in your organization? Have they all been configured securely? Consider one central FTP site.
- Who can touch your network?
    - Do you block all countries accept the United States? Consider this option to minimize who can get to your network. Certainly Russia, Serbia, Maldives, and other bad actor/nations should be blocked.
- Do you have a Data Security Agreement in place with all third party vendors obtaining sensitive data from you?
    - Make sure you include destruction/removal of that data from their system once your agreement ends. Consider certification of destruction.
    - Unfortunately, your data goes into the their backups and many vendors have no easy way to remove that data.
    - Be aware of companies being bought out by others. You will need a new data security agreement.
- Stress the importance of the need for a Computer Information Security Department.
    - Have regular IT security meetings.
    - This department is independent of other IT departments to make sure you keep everyone on top of what they need to be doing on computer security.
    - Remember, emphasize to leadership (Principals meetings, etc.) it is not a matter of if you will be breached, but when. Now the emphasis is on minimizing the amount of data loss.
    - The saying goes….there are those who have been breached and those who don't know they've been breached.