K-12 Privacy Leaders Working Group Meeting notes

Wednesday, December 6, 2017
11:30am-12:30pm
Topic: Security of Student Data Webinar

Speakers

- **Ross Lemke,** U.S. Department of Education's Privacy Technical Assistance Center
- **Lance Lennon,** Eagle Grove Community School District & the Iowa Technology & Education Connection
- **Amelia Vance,** Future of Privacy Forum

Ross Lemke on FERPA & Data Security

Key Points:

- Data will get breached (You're never going to be 100 percent secure. So, really data security is all about managing risk.)
- You will never have enough resources to be "secure"
- It is about how you prepare. (Ask this question → What are the risks inside of your organization are what steps are you taking to mitigate that risk?)

What specific technology controls does FERPA require for your IT systems?

- Nothing

Why doesn't FERPA tell schools how to protect student records?

- FERPA was written in 1974. Initially, it focused on the protection of paper records and information. This is both a blessing and a curse. FERPA addresses data security through the concept of "Reasonable Methods."

What is a reasonable method?

- FERPA evolves with technology. A reasonable method for 1974 might have been locking the principal's office or file cabinet. What's reasonable today could be encryption, robust passwords, or firewalls.
- We generally interpret reasonable methods to mean a set of security controls that are in line with current accepted security and privacy best practices for data of similar sensitivity.
- Points to remember:
    - Know yourself
    - Know your adversaries
    - Know how much risk is OK
    - Deploy the security controls to mitigate that risk to acceptable levels

Three pillars of reasonable methods:

- Technology (can be the easy part)
- Policies
- Training (can be more difficult when you get to the "person level")

Why are we even talking about data security?

- FERPA requires it.
- Students deserve it. (Can cause harm to students whose data are lost).
- A breach could cause reputational harm for agencies.
- A breach could cause financial harm for agencies.
- Electronic records are more prevalent than ever.
- We collect more, move more, use more, and lose more data than ever before.

What keeps me awake at night?

- Data Breaches. We hear a lot about data breaches at big retailers or insurance companies because those organizations are big and they have the technical capacity to know that they have a breach.
- Does a small district, where the IT staff might be the gym teacher, secretary, or vice principal, even have the technological skills or capacity to know that it has had a breach? The breaches that aren't reported are the ones that are really terrifying.
- Comparison of cyber-security budgets
    - Pentagon = $6.7 Billion (and still gets data breaches)
    - School district = Gym Teacher's salary

Problems in education data systems

- A ton of old or unpatched software
- Don't forget that IoT devices in schools include:
    - Server room cameras and sensors
    - School surveillance systems
    - Access card readers
    - Modems (UPnP hackable)
    - "Smart" HVAC/Boilers
- Hundreds of forgotten servers/computers
- **EXAMPLE:** A university in Wisconsin had their security cameras set up with no username or no password required to access the camera feed – so nobody's hacking into anything. All you needed to know was the website to see the camera, students, and the professor on the Internet. And this is a university that has an IT budget and security staff. Imagine you're a charter school or a school district that has only two elementary schools.

Problems in education data systems for one state found in one afternoon

- 626 machines that did not have a firewall.
- 2 SIS breaches affecting thousands of students
- Hundred s of anonymous FTP servers
- 143 Windows XP machines (some already hacked)
- 10 VPNs running out of date Windows 2003 Server
- 835 Web servers running IIS 6 or earlier

How do schools get hacked? How a school district is vulnerable?

- Back in the early 90s late 80s, you actually had to know something about computers to hack into things.
- These days it's really easy. You can google how to hack (there are tutorials), download packages, or go to the dark web and pay people to go build hacking tools for you. It's not hard anymore.
- <u>Google can be a hacker's best friend.</u>
    - A person can use google to look for files called web.config that have not been properly secured.
    - These particular files are going to reveal lots of sensitive information for us, specifically administrative passwords to applications, databases, and other assets. No hacking skills are necessary.
    - There is an online database of useful Google search terms. They're called the Google dorks of the Google hacking database. Using these things, you can spot misconfigurations, find vulnerable servers, discover PII, passwords, sensitive documents etc.
    - So, if your webserver is not set up properly there's the possibility that your web.config is left exposed where a bad guy can notice it/take advantage of it.
- <u>Phishing E-mails</u>
    - Most phishing e-mails are easy to notice. Here are some things a sophisticated hacker could do to gain access to your systems.
        - Locate staff directory (many school districts publish this on their websites)

        - Send phishing email to targeted employees, infecting the unwary user
        - Locate data, pawn everything
        - Profit

What are the threats to student data?

- Internal – Self-Inflicted Wounds (Mistakes, Intentional misconduct, Curiosity)
    - Falling for phishing email/clicking on stuff
    - Unsafe browsing habits
    - Use of "Free" WiFi:
        - **EXAMPLE:** Pineapples, which are devices that spoof Wi-Fi hotspots, are cheap and easy to obtain. At a recent conference, we set up a pineapple and named it "AT&T Wi-Fi." Within a minute, we had 20 devices connected to it, including the devices of people that were in our audience. If we were bad guys, we could mess with the Internet traffic, replace all the references of the news articles they were surfing, or show all the websites that attendees were visiting when they should be paying attention to our security presentations.
    - Misaddressing email
    - Sending attachments with PII (easy to do if there are two people in the same department with the same name)
    - Lost or stolen storage/hardware
    - Weak passwords
- External – Enemies at the gate (Hackers, Social engineering attacks, Malware)
    - Malware/Ransomware
    - Application hacking
    - Man In The Middle (MITM)
    - Denial of Service (DOS/Ddos)
    - Mobile/remote
    - Third-party attacks

Understanding the Threat

- Cyber criminals
    - Motivated by money
    - ID theft
    - W2 scams
    - Financial Crimes
- Employees
    - Just looking
    - Occasionally malicious
        - **EXAMPLE:** Disgruntled employee who fired deleted 1450 out of 1500 students from the student information system. They didn't not terminate his access to the student information system immediately when he was let go.
    - Fat fingers & bad habits
    - Whoops moments
    - Road warriors - people leaving their laptops set a Starbucks Target you know having stolen off the conveyor belt the TSA security of the airport.
- Hacktivists
    - Motivated by attention
    - Low hanging fruit
    - Defacements/DoS
    - Outing security fails

Security/Data Breach Pyramid for Student Data

Note: 0 Day Attack is at the top of the pyramid. It's a small threat compared to the others. Time/resources are best spent addressing the more likely vulnerabilities.

What is social engineering?

- The use of deception to manipulate individuals into divulging confidential personal information that may be used for fraudulent purposes.
- Phishing emails
    - Example: "Our web site monitoring tool has detected several attempts to access content at inappropriate websites. To review and provide a justification, please click on this link to prevent your log in from being disabled and your supervisor from being notified."
- Spear phishing & whaling (going after prominent person on the staff like a superintendent)
    - Example: 2017 W-2 Fishing. Here's how it works. The bad guy uses the internet/makes phone calls to find people in key positions and their email addresses. Once they have this information, they masquerade as a person of authority (e.g. superintendent). They send an e-mail to HR payroll employees asking for copies of W-2 before they go out. The unwary victim sends W-2 to the bad guys who then in turn files fraudulent tax returns with the IRS.
- Telephone calls/sms messages
- Baiting
- Watering hole attacks
- Scareware

How can schools combat social engineering?

- Train users on information security annually
- Training should include phishing/safe browsing habits like:
    - Being wary of unsolicited email from untrusted sources
    - Ensuring connections are secure
    - Validating links before clicking
    - Training Example: Many districts these days that are starting send out test phishing e-mails to their staff to see who clicks.
- Make sure employees know who to contact in the event of an issue
    - Mistakes happen. Have them have a culture in place so that employees know where to for help/encouraging them to ask for help because once you know about the problem you may be able to stop it before it becomes a major crisis.
- Do not rely on technology alone

What to do – organizationally

- Make good, reasonable policy that is backed by **leadership**
    - When does leadership usually consider something important in school districts? Unfortunately, it's usually after something bad has happened. It's our job to stress and make this a priority before something bad happens. If something bad has happened, it's already too

late. If leadership doesn't buy in, it's not going to be important. If your leadership is right, there with the staff taking that security training that can really highlight to the people at the ground level that this is so important that the superintendent is taking this right along with me

- Do a risk assessment, determine your risk threshold
    - The single best bang for the buck that you have for lowering your risk is training. And yes you send out the fishing you know to your staff. You might get 40 percent of your staff clicking on the first time while maybe the next time it's 30 percent or maybe next time is you know time after that's 20 percent. I think security trading multiple times a year probably three times as you know the Department of Education and several times do my own company in a lot of time just covers the same information. But eventually it starts to sink when you start to bring to develop a culture of awareness.
    - Training coupled with security awareness updates
- Develop an incident response plan
    - Train staff on the plan
    - Test the plan
        - At PTAC, we have data breach response exercises and checklists, that you can use to come up with your own plan. But once you have and it's in a response plan, it's no good if people aren't aware of the plan. It is important to train your staff and test the plan.
- Think like a hacker!
    - Ultimately think like a bad guy look at your own networks and your own people and think well if I wanted to hack myself how would I do this. What vulnerabilities would I focus on?

What to do – individually

- Use encryption. SSL/TLS, VPN, Full-disk, file level
- Verify website are secure by visually checking
- Treat all WiFi as untrusted WiFi
    - *Free WiFi* can be convenient, but using free WiFi carries some risks:
        - Fake access points can lure you into connecting to a hacker's system, esp. if your devices are set up to connect automatically.
            - **EXAMPLE:** Attackers can send a spoofed message pretending to be a "trusted access point" instructing the User's computer to disconnect. When the user disconnects, the attacker then creates his own access point with the same Service Set Identifier (SSID) (e.g. Free WiFi). The Client's computer then reconnects to what it thinks is the same "Free WiFi" network, and the Attacker becomes the ISP, enabling him to monitor and manipulate the user's network traffic. So, when school staff connect to free WiFi, this is an area of concern.
        - Man-in-the-middle attacks can expose sensitive data in transit
    - Security Tips
        - Avoid using untrusted networks to do sensitive things.
        - If you must, use Virtual Private Network (VPN) technologies to secure your access
        - Don't join wireless networks automatically or just turn off WiFi unless you need it.
        - Beware of odd behavior on free WiFi networks, like frequent disconnects, slow performance or certificate warnings.
        - Employ strong WPA2 encryption for own wireless networks with a long and complex paraphrase
- Use strong passwords
    - Zq4ab!ui – pass requirements too hard? People are going to write it down.
        - Takes 9 hours to crack this password (not very secure)
    - I L0ve my M0m! (easy to remember, don't have to write down)
        - Takes 429 billion years to crack
        - Think out ide the box (try sentences and phrases)
- Check links in emails and documents before clicking through them
- Never plug in a strange flash drive
- Set a screen lock

- Patch and update regularly, especially for third-party applications

PTAC= the good guys

- If you have a question, you can ask for yourself or you can ask for a "friend." Everybody makes mistakes. We just want to help you reduce those mistakes and help you get better in the future.

Lance Lennon on Account Security

Key Points:

Background on the Dark Overlord hack in Iowa

- What happened?
    - In Johnston, Iowa, parents started getting texts from an individual saying that their children were in danger. These texts specifically talked about how particular a student would be harmed during a particular class at their school. It was very disconcerting because it was not random. These were actually parents who had students in that school district. The hacker(s) also did a web dump, posting student names, student e-mails, student cellphone numbers, parent name, and parent contact info on the web
- Where did this information come from?
    - There's a little bit of discrepancy on where this information came from. The student information system the school used said it showed no breach of anything of any type. But it really got a lot of schools in Iowa to start thinking – "What do we need to do for account security for our teachers and for our student information systems to make sure that we're safe?" Note: Most public-school districts in Iowa have thousands of students and only one tech director.

Google for Education – What can we do to make sure accounts are safe?

- Use Google Two-Step Authentication (all cloud-based and local-based systems need to use two-step authentication)
    - Password Requirements
    - Limit API Access
        - **EXAMPLE:** Last spring, there was a hack that Google managed to stop within an hour, but during that time it had propagated itself - who know how many times. Someone got into the API and realized that so many people said, "Yes, I want to give this application complete access to all my information."
    - Use the Authenticator App
        - Teachers log in, go to the authenticator app, and put in the code that's there. The code changes every 60 seconds. The odds of someone having your username and the current code is hard (but not impossible).
    - Provide YubiKeys for teachers who don't have smartphones
        - Two-step authentication that requires a USB device. Teachers plug it in, and touch with their finger (not a finger print reader, but they have to have physical access to it for it to work).

    - We also allow teachers to have texts sent to their phone for two-step authentication, and some teachers use LastPass, which has two-step authentication built into it.
- Make Chrome our Default browser

    - It auto updates. It is tested over and over. Of the browsers, it is found to be the most secure. (Nothing is 100% secure).
- Set up Google reports.
    - If you are a Google for education school district, you can go into the report section and set up manage alerts to build custom reports to get information as to what is happening.
    - Manage alerts with alerts for Logins/Changes, Drive access/updates, and email logs.

Apple Security – What can we do to make sure accounts are safe?

- In your security and privacy settings, you should require a password on screen saver or when the computer goes to sleep so that if you walk away it doesn't let someone come in and start using your account.
- We also disabled the automatic log in, so someone has to use their password to get into their machine. If you get a hold of someone's machine, you can bypass a sleeper (a screensaver password) by restarting the machine if automatic log in is turned on, so that makes it almost a ridiculous security measure without the other.
- When you set up the screen saver to come on? The sooner it comes on the better.
- Set up Two-Step authentication with iTunes especially through your Apple ID. It sends out a code that they have to put in in order to actually access or to be able to install things on the computer.

Where did the dark overlords get their information?

- The student information system that Johnson was using claimed that they were not hacked, so how did they get that information?
    - It doesn't matter what state information systems they use (e.g. infinite campus, skyward), it is important to turn on/look into account access. In the past, parents found out about how their kids were doing through midterm reports. Now, parents can see how their kids are doing in school by the minute. Increasing access = increased opportunities for accounts to be compromised.
        - We audited our student information system (not only parental accounts but also user accounts) as to who had access to what, do they need that access, and really pared down some of the stuff we did. It's easy to just give everybody full access because they'll only use what they need, but if their account gets hacked then the hacker has access to everything.
    - The bigger problem is not so much what is your student information system, it's all the other things that you tie into it - whether it's through the student interoperability framework, API access, direct access to the database, there is a wealth of information that you really need to protect.
    - Many tech directors in the state believe the hack came from "a remind 101," where parents set up accounts and sign up to get the texts from teachers. This is probably an easier system to break into than Johnston's student information center. This make sense because every student in the district was not targeted – only particular students/parents.

So, how do you avoid getting compromised?

- Train your staff on
    - Social engineering

      All it takes is one person to fall for it to open the floodgates. One way is to "self fish" and if a teacher falls for it, suspend their account until they go through the training again. It's also important to train on a regular basis.
    - Brute force attacks
        - The more complex you go with passwords the more likely you are to write them down.
        - Keeper app. It's a secure app that I have to have the password to get into I can also use my fingerprint, but if I do three incorrect passwords it wipes all of that information.
        - Use phrases that you remember (phrases)
        - How secure is my password.net → Interesting. How safe is it to put in a bunch of passwords? Is there somebody on the back end just collecting a whole bunch of

passwords to use in some sort of brute force attack? But great information to have in finding out what it would take.

- Over the shoulder hackers
  - The person who is training themselves to watch your keystrokes to get your password, which is why the shift key becomes even more important. You know when you put it in certain words doesn't matter how fast you type someone will probably be able to over your shoulder find out that information. So, train them about using the shift key because that then completely changes what your password is based upon just keystrokes
- Keylogger software
  - We make our staff administrators of their computers so that they are allowed to install software, but once keylogger software is installed it's no different than someone putting in a skimmer and to get your credit card information that you log (scary/frightening because it's finding all that information that you are typing).

Questions & Answers

1. *When some districts address digital equity for students by suggesting that students access free area hotspots, is that not inviting challenges?*

- **Ross Lemke:** Yes, there is a constant tradeoff between convenience and access and, in this case, between equity and information security. Some free area hotspots are better than others (e.g. employing security or credentialing). It is important to think about whether students are giving out their PII on these connections. Students should also learn digital citizenship, including things that they should/ should not do on the Internet, passwords, and the basics of information security.

2. *Are the widely available VPNs trustworthy?*

- **Ross Lemke:** Avoid are the ones that are old and out of date. You want to do your due diligence on any tool that you're going to use. Oftentimes with software, there's other sources that you can use to look for vulnerabilities for particular types of software. (You can reach out to PTAC about this).
- **Amelia Vance:** I know one cyber security professional who uses VPN Unlimited. He noted that Google and Facebook who of course have a lot of reasons to make sure their employees do not have issues are using the Citrix and/or Cisco VPN and then open VPN is also widely used and is trustworthy.

3. *For policymakers and people who are trying to figure out their budgets next year, how should people spend the money they have to create better security? If they don't have that funding, how should they talk about the value of getting additional funding to build in additional security?*

- **Ross Lemke:** Use examples of data breaches from within your state when trying to explain the value of getting additional funding to build in additional security. Here are school districts within our state that have had data breaches. Explain why the data breaches are caused (e.g. lack of training, phishing, etc.) Explain the costs associated with data breaches. If the training that you do just stops one single data breach, then it's paid off. The costs of data breaches include reputational harm, identity fraud, potential FERPA violations, etc. are going to be larger problems for your school district.
- **Lance Lennon (addressing the budget question)**: All too often in our state, budgets are constantly declining and trying to do more and more with less and less. Schools may want to consider:
  - **Audits by security experts** = money well spent, even if it taught me that I had done things right so at least I know that I'm doing things correctly.
  - **Insurance for data breaches.** A lot of school districts don't even know that exists. do you. If something does happen, schools would be liable for information that got out and damages that are occur because of that
  - **Equipment.** Firewalls are important to have and maintain (e.g. patches) and VPNs.

4. *What is the value of cyber insurance? What does it cover?*

- **Lance Lennon:** I would recommend looking at it. Talking to your school's insurance carrier to learn about the cost and what it would cover. It's a good conversation to have even if you do nothing with it. It's the best conversation you ever had if you ever end up needing it.
- **Ross Lemke:** As I've gone into the field, I've heard more but more about districts going this path. I think it's sometimes regional. I see it a lot in certain states. The real question is going to be down the road when people start having data breaches - what happens when they try to use the insurance? I can't speak to the services, whether they are good or bad.

5. *How do you communicate with communities about hacks?*

- **Lance Lennon:** Because our school district was not affected, we had time to put together a nice communication to our constituents, our students, and our parents in regards to things that we do have in place and that we take their security and their information seriously. We sent that out. We also have a monthly newsletter that goes out and we were able to a messenger app to send out information to parents.
- **Ross Lemke:** Don't be disingenuous. Don't say, "We're going to go review our policies and ensure this doesn't happen again," if you don't review actually your policies or train people on the policies then is going to happen. Be transparent. If parents don't know what's going on with their children's data, they are going to assume the worst. It is important to be able to say what you are doing with the data, how you are protecting the data, here's who you can call if you have questions, etc.

6. *What are the security issues that can come up with external apps and how can you minimize those security risks?*

- **Lance Lennon:** In our district, we allow all apps except for the ones that we block. So, I'm consistently looking through and trying to find new apps that we don't want our students or our teachers to have access to. We don't run anything via student interoperability framework (SIF), but if you choose to do so (e.g. a third-party tool that's connecting to your student information system, your active directory, or your cloud based directory), look into/determine → what is it they are really getting, what are they doing with that data, and how much control do I have? It's also important to have audit logs so that you can look through it to see what happened, who did what. and when. If nothing else, it's is what I call a "CYA policy," which covers you so that you can show that you were not at fault.
    - **EXAMPLE:** Pokémon Go and lazy coders - all they did was use an older Google API. People love the simplicity of a single log in (e.g. through Facebook or Google). So, the coders just used an old API to get access to everything inside of your Google account. The risk is considerable. I mean how many times do we just click, "Yes, yes, yes," during installation without reading because we want the installation process to be over with. What you are you actually granting access to?
    - **EXAMPLE:** Before purchasing Go Guardian, I told the company I needed to be able to prove that I am not accessing student webcams when I shouldn't be. So, the company put audit logs in. An audit log not only helps you know what a third-party tool does, but it also gives you an audit trail to show that that you did everything right.
- **Ross Lemke:** Having something in the cloud could potentially be more secure than what you have on your own networks. Our expectation is that any cloud service provider is going to have the at least the same level of security. But ideally it's going to have better, if it's a really good service. I think your biggest concerns come with some of these new apps out there (e.g. Pokémon Go). There's also issues with user agreements (e.g. ones that may put them in odds with FERPA regarding data ownership) or it could be a service is not going over HTTPs so that that's probably an issue. A lot of it's just doing your homework with these services.
- **Amelia Vance:** Privacy best practices include making sure teachers know not to fill in things like optional fields (as they're signing up for apps if they're allowed to do so in your district) and making sure that there is the minimum information out there, so if there is ever a problem you don't have a whole lot of information that has been breached.

7. *How can you minimize threat from students on your network?*

- **Lance Lennon:** It’s a huge balancing act because you want students to learn and you want them to have access to tools that they're going to have access to in the real world. So we
    - Ingrain (as much as you can) the idea of digital citizenship, proper use.
    - Mitigate risks in terms of not giving them carte blanche access to your systems
    - If I find a kid that has that kind of drive to learn these kinds of skills, I try to help them pursue a tech career (positive vs. negative use of skills).
- **Ross Lemke:** If you wanted to eliminate any risk of students doing something bad, you would not give them access to anything, which of course is unreasonable. So it’s a lot of balancing. There’s always going to be some element of risk with what you do. It is important to understand what your risks are and reduce your risk to a level that is acceptable for your organization.