Cybersecurity in Education

On **March 27, 2018**, **James Costello, Eric Pina, Derly Buentello, Kimberly Osborn** and **Jennifer Miller** attended the workshop Cybersecurity in Education.
David McGeary welcomed the audience to the meeting. Attendees included many districts in Harris County.

James Morrison, FBI

The private sector is the key player in cyber security. Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to address cyber intrusions and cyber crime in general. - Former FBI Director, James Comey

Schools are a target for cyber criminals. Are we focused on what is important and what we need to ensure is protected? We need to have the mentality of what could go wrong and are we planning for what we will do when it occurs. Planning is a big part of cybersecurity. The audience was challenged to have an answer for the question "What is your plan?"

90% of cyber attacks begin in universities. Kids are learning to program and get paid to attack.
The Actors

- International – State Sponsored and criminal Enterprise
- Domestic – Criminal Enterprise and Others (Hacktivists, Joyriders, etc)
- Internal – Insider Threat

Internal threats are our biggest challenge

- Malignant and uneducated users
- Biggest challenge is the length of time it will take you to find the internal threat.

James Morrison

Cybersecurity in Education

Current Threats

Website Defacing – student defaces the website. Must make sure that we are protecting websites from infecting users devices.

Distributed Denial of Service – (DDOS) – disrupts ability to use devices. Criminals use district networks to attack other networks. We must protect our network,

DeOS – next phase of attacks - destruction of data if ransom is not paid. Destruction of data and computer hard drives.

Phishing – spear-phishing, whaling, vishing – voice call phishing, SMS phishing (smishing)

limit what people can see or do on your network

75% of phishing attacks come from oversees. Many come overnight. Target the training to train those coming in early to spot the issues.

Ransomware – usually begins with Phishing e-mail or other Social Engineering Attack

Backups are critical, if infected, backups may be the best way to recover critical data.

Ensure you have robust backup and restore procedures.

Secure backups offline.

Stop sending a link or attachment – Have a protected website that you ask the customer to login to access.

Phishers look at social media sites to collect credentials

Have someone watching your social networking

Talk to other school districts to share lessons learned.

The Internet of Things (IoT) – thermostats and multiples of things – ensure your network is secure.

James Morrison

Cybersecurity in Education

3 ways Data Gets Lost - Data at rest, in use and in transit.

Final Reminders

1. Need to teach kids how to protect their data – freeze kids credit at the earliest age to protect their SSN
2. Good idea to pull your data from Facebook and review periodically
3. We must have a plan for cyberbullying. Kids that are getting physically bullied at school are attacking others through the internet after school. Sometimes best thing in cyberbullying is to remove the device.
4. Parents and Teachers need to be aware of what students are doing on their phones.
5. Public wifi is not safe – do not use public wifi for personal or corporate firewalls.
6. Ensure that passwords are changed frequently.
7. Have a banner that says “logging into this network allows consent to tracking”
8. Password vaults are a good idea
9. Antivirus and passwords should be kept up to date
10. Must have encryption process – data at rest should be
11. encrypted. Then unencrypted at use and then re-encrypted.

Cybersecurity in Education

Data Privacy & Protection – The Basics (in Plain English)
Mary Dickerson, University of Houston

Schools handle man pieces of Protected Data!!

- Information protected by law
- Information protected by contract
- Passwords and other authenticating information
- Information considered by its “owner” to be private or sensitivity

By themselves, small bits of data, but when you put it all together it is quite serious.

Impacts can be significant

- Financial Loss - may need to setup call centers or send out information – all adds up
- Loss of reputation – biggest impact
- Criminal Prosecution

A few things that keep an Information Security Officer awake at night?

- How much protection does our information need?
- Are we doing enough to protect it?
- How do we balance risk and cost?
- Does everyone know what he or she has to do?
- **Do they understand why?**
- What kinds of information do we have?
- Where do we keep our sensitive information?

Mary Dickerson

Cybersecurity in Education

Important that when you tell people what they need to do that you explain why they need to do it.

Addressing Your Cybersecurity Info Risks

Don't keep information you don't need
Use Current Forms/Documents
Know what data you have and where it is
- Who are the Business Owners?
- What are the Compliance Requirements?
- Standardize Storage Locations & Protect
- Document incident response procedures
- Empower your Employees!

Eric Pina

Derly Buentello

Employees are the front line of defense!!!!
Leverage industry experts – FBI InfraGard, ISSA, ISACE - http://cyerhouston.org
Cybersecurity Preparedness Assessment
Cybersecurity for the Board of Directors
http://www.texascisocouncil.org
Information Security Program Essentials
37 page guide is a back to basics approach for information security management and is a "Step In' simplified framework.

Harris County Department of Education

Mary Dickerson

Cybersecurity in Education

IMS Global Learning Consortium Digital Literacy: A Tale of Two Worlds
Kevin Lewis Sr.

It was the best of times, it was the worst of times.
This is a great time to be alive with all of the technology available, however It is also a time that we need to be concerned about the security of our data.

He reminded the audience that apps are free – just like a puppy. However, like a free puppy they require much care.


Kevin Lewis Sr.

He shared the process he embarked upon while working with HISD in reviewing the ratings of multiple internet apps. It is important that school districts continue to remain informed about the apps in use in their district. Application vetting processes - SSLLabs

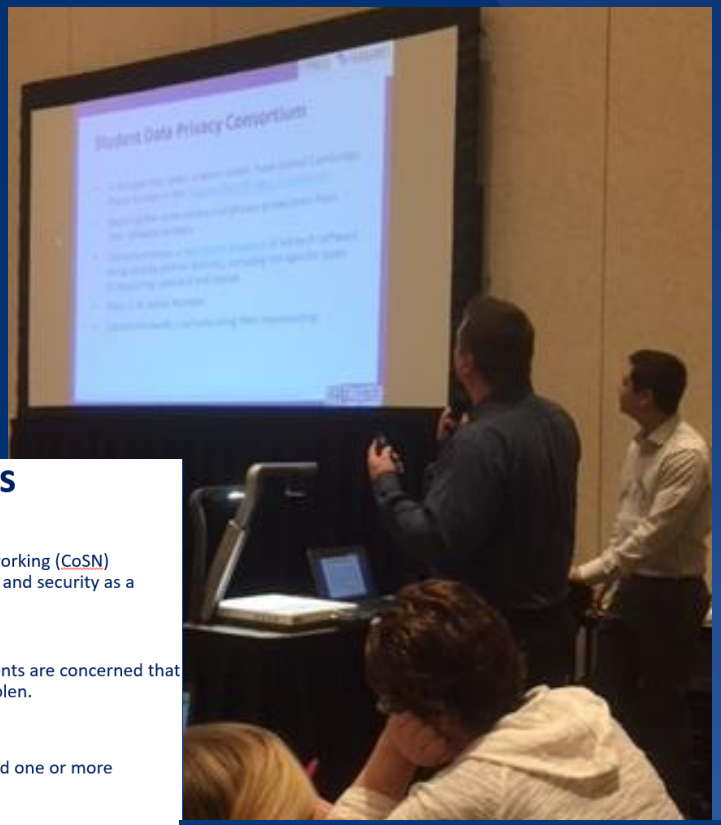
Why You Need An Information Security Advisor
Christopher Kar – Fort Bend ISD
Mr. Kar shared his experiences in a K-12 environment. He shared many key points of items that make a successful cybersecurity team.

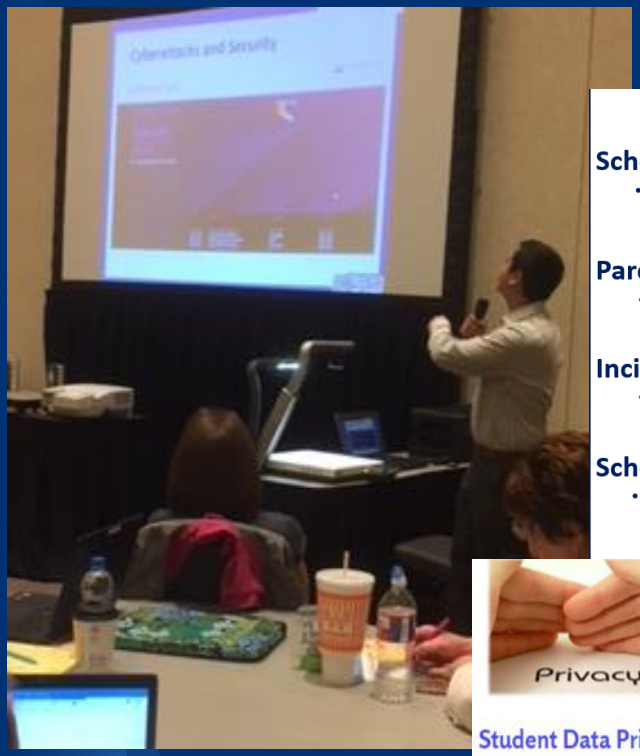
Acceptable Use Agreements
Content Filters - Is 13? / Is 18? – allows filter to be set based on age. . . .
Proxies / Filter Avoidance
SSL Decryption

Christopher Kar

Cybersecurity in Education

On Thursday, March 29, 2018, James Costello, Eric Pina, and Jennifer Miller were invited to present information to the District Librarian Meeting. The team presented information related to the Trusted Learning Environment Seal application. The Librarian team has been very helpful in gathering information related to lesson plan information. The Librarians asked great questions and were very excited about the upcoming KnowBe4 training that will be distributed during the week of April 2, 2018. The Librarians will be the second instructional team to receive cybersecurity training.





Privacy and Security Concerns

School System Leaders Are Concerned

- According to the results of the 2017 Consortium of School Networking (CoSN) Leadership Survey, **61%** of technology leaders identified privacy and security as a primary concern.

Parents Are Concerned

- In the 2016 Future of Privacy Forum survey results, **84%** of parents are concerned that their child's electronic education records could be hacked or stolen.

Incidents Are On the Rise By 100%

- Since 2016, hundreds of K–12 schools and districts experienced one or more publicly disclosed cyber incidents.

School District Must Take Action

- In 2016, an audit of some 1,200 web-based education software products by the nonprofit Common Sense Education found that nearly half the offerings didn't automatically encrypt student data.

Click here to view the presentation

Student Data Privacy

Cyber Security Current Events

Cyber Security Awareness

KnowBe4
Human error. Conquered.