Review for Presentation

1. Kentucky's data privacy laws, what constitutes a breach (your Board Attorney should be up on this, too),
2. what sorts of data the district works with (it's MORE than just student PII – can include teachers, parents, network diagrams, etc.),
3. what data systems exist (e.g. MUNIS, IC, Cafeteria, Library) and who or what entity is responsible for their security (external vendor, KDE, or the district), and are they backed up? What happens if local data systems are flooded or internet goes down? Can "school" still happen?
4. what you believe the risks in your district are (e.g. had a phishing problem? Crypto-locker? Weak passwords?) and
5. what the district is doing NOW about security risks (e.g. strengthen passwords, awareness campaigns, trainings, friendly phishing campaigns, discipline, DMARC/DKIM, Data Loss Prevention, HD encryption, external email banners, safe links, safe attachments, home network security awareness given the move to NTI),
6. what you plan to do about security weaknesses in the near future (MFA, address stale accounts, implement MS A3 or A5 with data loss protection, message encryption, etc), and what you would LOVE to do about it but cannot right now, and why (money, manpower, staff pushback, etc)

As a quick "for instance," let's say your district folks have a problem because they need to be able to send top secret information to a vendor or between schools, but get nervous thinking about sending it via email (which IS risky and not recommended) but you don't have the budget to purchase the A3 Office 365 license from MS, which would give you email encryption, then you would want to let the board and district leadership know that the district has a risk and a gap there. What's the cost to remediate? What's the potential cost NOT to in terms of data breaches?

It could also be that you don't have enough staff to respond to all the crypto-locker happening in the district, since you have to wipe each computer and restore it. You might want to explain that you wish you could remove all the Local Admin Permissions from 90% of workstations, or that you plan to do that next year. What's the broken glass? Is there a cost to do that?

There are ALSO LOTS of potential items that you can identify both as WINS that you want your board and leadership to know about, and as RISKS or LOSSES that you want to bring to their attention. Definitely do NOT forget to list the WINS. SO MUCH of security goes on behind the scenes and no one knows it's happening. Folks NEED to KNOW, but you don't want to list details in a public forum so crooks will see what you've got and what you've not got.

There's no set length or even format. Could be a sheet of paper or 50 pages. Or, you could just tell them face to face, and if they have questions that you aren't able to answer, just say "I'll have to get back to you."

In my own report out, I try to provide a summary of the following:

1. Number of data systems at KDE
2. Number of those data systems that contain PII
3. Number of those data systems that contain SSNs (a subset of PII, but an important one)

Jefferson County Public Schools

Digital Privacy, Safety, and Security

August 2024 Update

JEFFERSON COUNTY PUBLIC SCHOOLS

JCPS™ IT3

Information • Integration • Innovation

How does JCPS IT Identify, Mitigate, and Manage Technology Risks?

Risk Management Framework driven by NIST

Continuous Improvement Efforts - assessments and collaboration

Technical Systems and User Awareness

Achieve balance of digital safety, privacy, and security for JCPS students and staff while supporting instruction and daily operations.

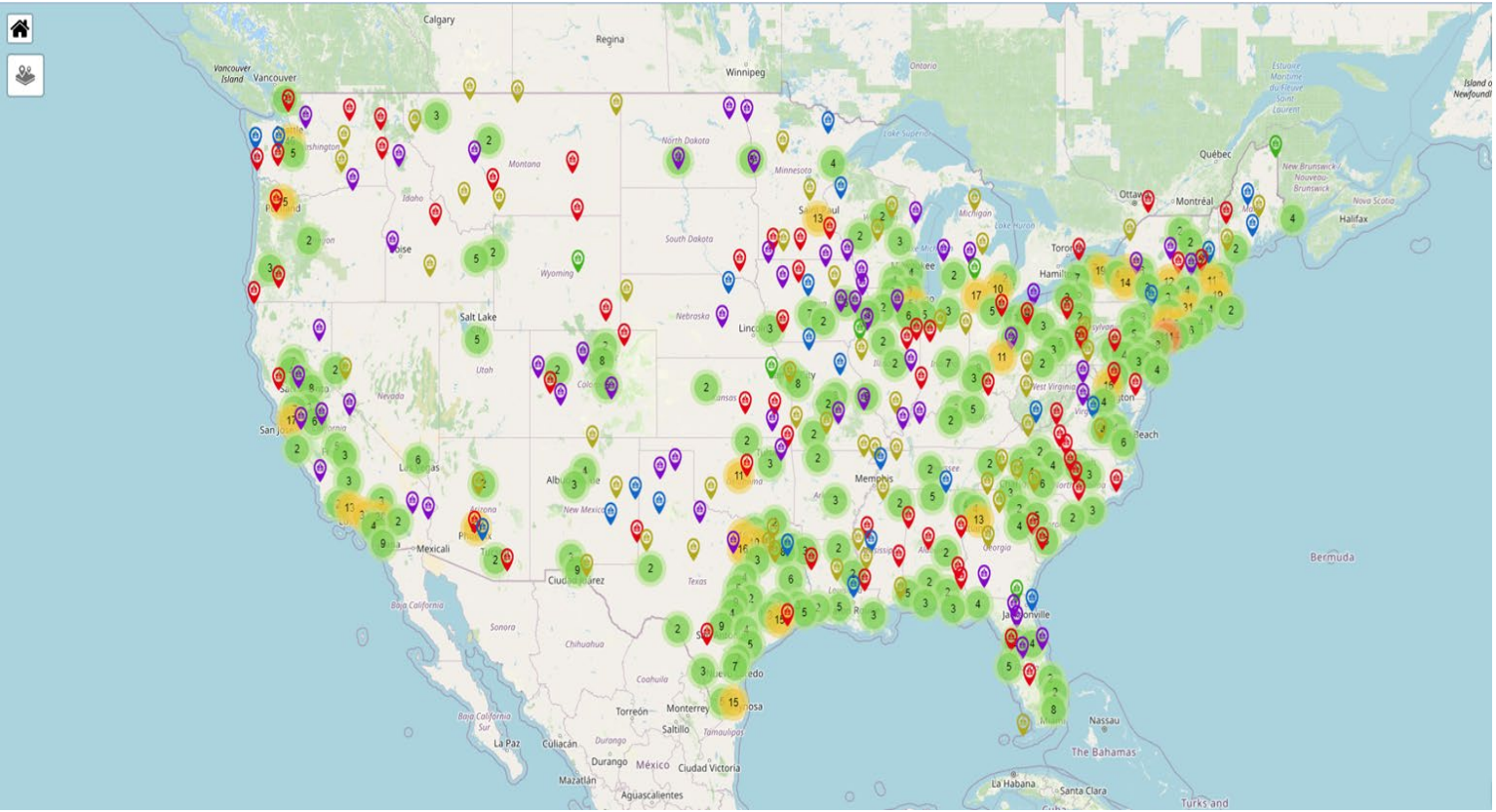
Increased Cybersecurity Risk

- Research shows that Education is the most aggressively attacked segment, in the second quarter of 2024, it showed 3,341 attacks a week on average, 60% more than the next highest segment of Government/Military. (Checkpoint Research)

- Phishing continues to be the most common attack vector, a suspected 3.4 billion phishing emails are sent every day. The use of stolen credentials through these attempts are the most common cause of data breaches. (AAG-IT.com Phishing Statistics)

- It is estimated that 59% of organizations were hit in the last year, with 70% of attacks resulting in data encryption. (Sophos State of Ransomware 2024)

Map of Cyber Incidents against K-12 Districts from 2012 - 2023



Legend:

Red - Incidents resulting in disruptions and unauthorized disclosures

Purple - Unauthorized disclosures, breaches, or hacks resulting in disclosure of personal data

Blue - Phishing attack resulting in disclosure of personal data

Yellow - Ransomware attacks

Circles represent groupings of incidents.

1,619 Incidents tracked by K12SIX

IT Risk Management

- Policy and Procedures aligned with the National Institute of Standards and Technology Cybersecurity Framework
- Maturation of the District's Digital Resource Review process
- Living Risk Register
- Partnering with CISA to improve the district's security posture

IT Risk Management
Continuous Improvement Efforts

Technical Controls

- Microsoft A5 - Defender for endpoint, Defender for cloud applications, phishing attack simulations, data loss prevention
- Google Workspace enterprise solution
- Single student and staff identity management solution
- Identity protection with dark web monitoring of JCPS owned identities
- Increased device security baseline with InTune in testing
- Implemented SIEM for the district
- DMARC/DKIM for increased district owned email security
- Vulnerability scanning for district data center

IT Risk Management
Continuous Improvement Efforts

Human Behavior

- Digital Privacy Awareness Training
- Industry Standard Phishing Simulation Exercises
- Digital Citizenship Curriculum

Organizational Coherence

- IT Risk and Compliance Governance - Matching NIST Policy and Procedures to actively identify and remediate non-compliance
- Engagement with Federal organizations to improve incident response
- Third-Party Management with District-wide Digital Resource Review
- Focus on continued improvement to JCPS SOC

IT3 Risk Management
Systems of Awareness

- IT / Internal Audit Risk Assessment
  - Targeted vulnerability Assessment
  - Microsoft and Google Domain Assessment
  - Windows Device Security Baselines

- Network and application analytics, security awareness
  - Vector Training
  - Network analytics
  - Threat Intelligence Feeds

Closing Remarks / Questions