Kentucky K-12 Experience and Recommendations on Cybersecurity

On behalf of the students, educators, the Department of Education of the Commonwealth of Kentucky, and myself, thank you for this opportunity to testify today and to answer questions you may have on the topic of cybersecurity and privacy from a statewide K-12 perspective.

At the Kentucky Department of Education, we firmly believe protecting student data is crucial and everyone from the classroom all the way up to the state department of education level has a meaningful role and responsibility in cybersecurity and data privacy. While we do many things from a pure technology perspective to provide cybersecurity at the state and district level, we spend more time on professional development, or what we call the "people side" of cybersecurity and privacy.

There were over 4 Billion attempted unauthorized network connections, or attacks, of KY K-12 services this past school year. However our biggest vulnerability by far is internal staff, not external criminals. We get more than our fair share of phishing emails and ransomware attempts. Kentucky K12 has implemented a great deal of technology solutions to limit these attacks. We very early realized that we can't expect our educators to be cyber-security specialists, however everyone has a role to play in maintaining security. Thus we must have each student, teacher and KY K-12 leader to be aware of the importance and their role in cybersecurity and privacy, as well as being very savvy and good digital citizens. We also believe our KY K-12 students and teachers can be innovative while at the same time respecting the importance of cybersecurity and privacy. Lastly we believe and support that some of the laws (e.g., FERPA) around data security and privacy need to be updated and modernized to recognize a technology immersed environment in K-12.

For the past 2 decades, I have been the Associate Commissioner for the KY Dept of Education (KDE) and the KY K-12 Chief Information Officer. I am the longest serving state level CIO of K-12 in the USA by a wide margin. Before coming to KDE in the early 1990s, I was an Army officer in a senior leadership position in creating and managing the Army's most modern cyber-intelligence facility at that time.

So I can tell you with confidence that KY K-12 has been the pioneer and national leader in most aspects of K-12 education technology from a statewide perspective. Included in the appendix is a brief video summarizing Kentucky's progress and how that has enabled student success. Therefore, we've had the Internet, cybersecurity, large scale data systems, instructional technology, and electronic communications on our radar screen much longer than anyone else. So hopefully we can provide some words of wisdom for other states to learn and benefit from. However that is not to say we don't or can't learn from other states. We do. I find through CCSSO's state Chief Information Officer (CIO) Network, most of my K-12 state level peers in other states don't look at each other as competitors but instead try to help each other in all aspects of education technology, including cybersecurity and privacy.

Here are some of the major accomplishments of the Kentucky Education Technology System (KETS) since 1992 that impact cybersecurity and privacy.

- In 1990s, KY K-12 became the first state to provide high-speed Internet access to every district. Also in the 90s, Kentucky was the first state to provide a common statewide financial management, student information system and email system for every district.
- In the 2000s, KY became the first state to connect every district office and school by fiber as well as the first state to meet the national goals for Internet speed per student.
- Beginning in 2009, this level of Internet quality and capacity to every KY district in the state permitted KY K-12 to become the nation's leader in cloud based computing for all our major instructional and administrative technology enabled services for school districts. This approach has not only saved us millions of dollars each year but has also significantly improved our digital security and disaster recovery readiness.
- In 2011, KY K-12 created the nation's first Digital Driver's License (DDL) for our KY K-12 students & adults to help them be good digital citizens. Districts from 49 other states now use KY's DDL.
- In 2014 implemented a robust and improved statewide Internet safety and content management service for all 173 districts designed to give them the ability to tailor web access in their districts for students, staff, or the public.
- In 2015, KY K-12 created a comprehensive cybersecurity best practice guide based upon reviewing and including some of the best practices of the other 49 states.
- In 2016, KDE created a 1 pager for K-12 teachers and staff to keep handy in paper form by their desk and in electronic form to help them better understand PII (which we informally call top-secret data), data breaches, and how to prevent them
- The "It Could Happen to You But Don't Let It" document is educational for our KY K-12 CIOs and edtech leaders; mainly to help prevent something bad from happening again in their district by making all KY K-12 CIOs aware of what breaches are happening/not happening in other KY districts, KY institutions, KY state agencies and other states around them. This tool helps make the importance of data security a reality versus a theoretical unlikely possibility to our district edtech leaders. It also helps motivate them to not let the same thing happen to their district. We use this document frequently when talking with Supts and KY K-12 CIOs/edtech leaders.
- Every district, no later than each August, must provide an annual cybersecurity health check to the Superintendent and their local school board. In 2015, the Kentucky Department of Education enacted a regulation that requires KDE and every district to review data system security and report findings to their respective boards of education. Promoting transparency in this manner has the effect of requiring districts to actually know what data systems they had, and what data were stored in each one, and then to have discussions about what security was or was not in place, and why, such as not enough funds. This allows for frank, thoughtful discussions about risk and where to assign resources for the greatest bang for the buck.
- Every district superintendent submits to the Kentucky Department of Education annual assurances relating to the 9 elements of Digital Citizenship and Cybersecurity (among other technology related items). We have found, in many districts, this provides an open

dialogue among school district leadership teams and increases strategic planning. More states should take this approach.

- We are the only state who has a monthly interactive webcasts for KY K-12 CIOs/edtech leaders, an annual KY K-12 CIO Summit that spends 95% of the time getting feedback from district CIOs/edtech leaders and DOE edtech staff in the field assigned to work with and help districts. KY Dept of Education's Education Technology staff regularly get invited by districts, educational co-ops, Kentucky Supts (KASS), Kentucky K-12 edtech leaders (KYSTE) Kentucky School Board (KSBA), Kentucky School Administrators (KASA), and other statewide organizations to talk about cybersecurity and privacy in K-12 in Kentucky pretty frequently. This speaks to the continuing relationship and TRUST in education technology that we've built at the KY Dept of Education level and have maintained with our districts over the course of more than 2 decades.

Additionally, we require our statewide edtech vendors to agree with a signature that they are aware of and will abide by Kentucky's data breach notification and student data privacy laws, which went into effect in 2015. Based on the recommendation of our state auditor, we require many of our vendors to provide unedited audit reports to us, so we can see how they are doing.

We have put KDE on a "healthy data diet" so that we collect only the data that we know is necessary, which has the side effect of improving data quality, which researchers love, and minimizing our attack surface. We regularly encourage our districts to do the same.

A healthy data diet also means only seeing the data you really need to see. In the military, we called this "need to know." We don't want to provide extra permissions to people who don't need them because it was easier or because of someone's feelings were hurt when someone else had a higher level of permissions. We help folks realize that fewer permissions is actually better, in the long run. There is also a big difference between need to know for your job and being overly curious or nosy that we regularly educate and remind folks of.

Perhaps because of all the other measures we've taken, the greatest number of data breaches in KY K12, by far, are either accidents, such as posting PII onto a website or sharing a spreadsheet with hidden columns of SSNs, or from lack of savviness of staff who fell for phishing scams like "your mailbox is over its limit – hand over your password." Professional development and awareness are the only solutions to this issue.

Because of our high degree of data quality and standardization, researchers often seek us out for research studies. We have to walk a fine line between wanting to help, and the responsibility to our students to keep their data secure for when THEY need it. While I'm sure that most researchers are very responsible, we always have concerns where they want to keep very personal data for years or forever, without appropriate regard for safety, security or the law.

While Kentucky has invested a great deal of time and resources into securing our environment, there are still some improvements we'd like to see at the Federal Level.

- It's just too easy to get data and there just are not sufficient penalties to make people care about the security of data that isn't their own.
  - Update FERPA to include vendors along with districts and schools.
  - Add meaningful penalties and fines to FERPA for an organization and any subcontracting organization, that receives top secret data and subsequently exposes the data, and
- Require more succinct and to the point human-speak Terms of Service and Security Policies from all vendors.

In closing, while we believe in and support the technology that can help keep our students, staff and their data safe, we believe even more in those very people, who, when armed with the right amount of awareness and care, can really make the difference in this fight. Thank you and I look forward to your questions.

Appendix

Responding to the requests of our human network, we provide professional development materials and handouts on a constant basis as well as security presentations at district, regional and statewide events. Meaningful professional development is a KEY component and one that we are still working to perfect. Some of the tools or resources we provide to districts have been provided to you as well on an accompanying document. Overall, this is a short list of the MANY documents/tools we have created over the years, including presentations, to help folks develop an understanding of how technology and the human come together to "be" secure and not just ignore the problem and hope it goes away.

- **The Kentucky Education Technology System (KETS) Story**

  KY K-12 is the pioneer and national leader of many aspects of K-12 education technology. This 1.0 version of the video, still under production, summarizes our timelines, successes, and how KETS has impacted the educational and administrative aspects of Kentucky's districts. https://vimeo.com/256828929/d41c8d812c

- **The KETS Greatest Hits Album.** The 25 year timeline of historic achievements of the

  Kentucky Education Technology System (KETS). See the attached document titled "History of Edtech".

- **1 pager for KY K-12 teachers, leaders and staff**

  This security awareness document is designed to be informal and eye-catching in order to stand out. We've attempted to simplify the many different types of sensitive or confidential data to just "Top Secret," which is easily relatable. We encourage the district CIOs/edtech leaders to break the document up into even more easily digestible chunks and email those out to their staff on a weekly basis. See the attached document titled "1 pager Top Secret Information and Data Breach Awareness".

- **Digital Driver's License (DDL) and Digital Citizenship Guidance for KY K-12 students, teachers, staff and leaders**

  Digital citizenship is a key component not only of maximizing use of amazing electronic resources, but using them safely and securely. Kentucky's Digital Driver's License is an online course that helps students and staff learn responsible and appropriate use of technology and prove they understand the nine elements of digital citizenship. The KY Dept of Education's Education Technology staff, working with the University of Kentucky and some of our district edtech leaders, created the nation's first DLL. Our DLL is now used in 49 other states. Below are links to the DDL, with links to multiple articles, and KDE's page on digital citizenship best practice for districts.

  http://idrivedigital.com/
  https://education.ky.gov/districts/tech/Pages/Best-Appropriate-Use.aspx

- **"It Could Happen to You But Don't Let It"**

  This document is a constantly updated security awareness document intended to make very clear that data breaches DO happen throughout Kentucky's educational ecosystem, and not just to giant multi-national corporations. Because most data breaches in Kentucky K-12 have been the result of simply not paying attention, pulling the information about those breaches together can help districts focus. This document is used frequently throughout the K12 environment and at every level. See the document titled " It Could Happen To You But Don't Let It".

- **2018 PII Check for KY Dept of Education Staff**

  Because we are big on securing the human and helping staff to take responsibility for themselves, in addition to technical measures to prevent data breaches, the Office of Education Technology also uses this document to ensure staff are aware of the risks of holding onto PII on purpose or accidentally. Like nearly all of our documents, it isn't super-detailed, but that's on purpose in order to try to prevent folks from "tuning out." See the document titled "2018 KDE PII Check".

- **Data Security and Breach Notification Best Practice Guide**

  In addition to simplifying 18 pages of legislated "have to" process instructions from KRS 61.931 et seq. (Kentucky's data breach notification law) down to 1 summary page for easier consumption, it clarifies the process that state agencies, including KDE and the districts, must use when sending notification of data breaches.

- **702 KAR 1:170 School District Data Security and Breach Procedures**

  This regulation, promulgated by the Kentucky Department of Education,
  Requires districts to report to their boards, annually by end of August, what they have done to mitigate breaches, and what they have not done (usually due to functionality requirements, cost, or other resource limitations).

  Requires KDE to report the same information to our Board

  Incorporates, by reference, KDE's Data Breach Notification and Best Practices document, also attached, into the reg.

  Requires districts and KDE to use a KDE-provided email distribution list (DL) when reporting data breaches. Because Kentucky law requires multiple state agencies to be notified of data breaches, this DL simplifies the process during what could be a stressful time.

- **Our monthly KY K-12 education technology leader's interactive discussion for all 173 districts**: http://mediaportal.education.ky.gov/technology/district-technology-leadership-webcast/

- **Our 2018 KY K-12 Education Technology Infographic:**
  http://education.ky.gov/districts/tech/kmp/Pages/S-and-R.aspx