**Q4 -** Are you finding value with CISA external vulnerability scans? **Yes/No**

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Count -  Yes: 1     No:2 not useful  3 have not ran it at all |
| Table 2 | Count -  Yes:  1    No: 5 no’s not aware, no reports where in use so hope it’s helping |
| Table 3 | Count -  Yes:   3   No: 3 (need assistance with interpreting reports) |
| Table 4 | Count -  Yes:  5  No:  |
| Table 5 | Count -  Yes:  5    No: Even though it may not provide a ton of info, but its a free service so it might as well be utilized. |
| Table 6 | Done one? Count -  Yes:  7    No: 1; Value? Count - Yes: 6.5  No 1.5. Greatest value is in primarily in the first scan. Subsequent ones are less helpful.  |
| Table 7 | Count -  Yes:  5    No: 2 |
| Table 8 | Count -  Yes:  6    No:  We all find value in CISA |
| Table 9 | Count -  Yes: 7     No: 0 Kenny and the security team shout out! |
| Table 10 | Count -  Yes: 4     No: (2 not sure) |
| Table 11 | Count -  Yes: 6     No: 0  —Made me feel like we were in a good spot.  |
| Table 12 | Count -  Yes:  5    No: 2 The ‘no’ would just be those having not signed up or not having received their first scan results yet. |
| Table 13 | Count -  Yes:  4    No: 0 - Provides a sense of comfort having it done knowing you’re in good shape..  (Be more beneficial to me to know what the report says). |
| Table 14 | Count -  Yes:   4   No: 2 (these districts are not using) |
| Table 15 | Count -  Yes:  5    No:  1 undecided as new on the job. |
| Table 16 | Count -  Yes:   7   No: Huge asset for districts and great information provided in the follow up when Colin came to the district for a one on one.   |
| Table 17 | Count -  Yes:   5   No: 0- Very valuable but verified the things we already knew. Weekly report is a good healthcheck.  |
| Table 18 | Count -  Yes:  2    No: (rest have not signed up yet)Gives a good report back, easy to read, if there is anything they scan that is needed |
| Table 19 | Count -  Yes: 6     No:   No brainer.  Definite value |
| Table 20 | Count -  Yes: 6     No:0  |
| Table 21 | Count -  Yes: 5  No: 1; not yet implemented, but on his To-do list |
| Table 22 | Count -  Yes: 3     No:  3   (3 have done it, all got value even if just CYA or confirmation)3 have not done it, but intend to - just haven’t gotten to it yet |
| Table 23 | Count -  Yes: 7    No: 0 |

**Q5 - Tell us the best security big idea from your table that you’ve implemented that you believe could and should be implemented across KY K12.**

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Running phishing campaigns against staff |
| Table 2 |  |
| Table 3 | Implemented a group-based (Distribution List) for staff to contact with any security related question, instead of emailing/texting an individual for assistance.  Also implemented standard operating procedures (like a runbook) on how to manage/contain compromised accounts. |
| Table 4 | Containing schools so that if there is a breach, it’s contained.  |
| Table 5 | Better App management on almost a daily basis.Privileged identity management in Azure. |
| Table 6 | Conversation shifted to desires, rather than successes. MS A5 licenses are needed to allow for all users but are prohibitively expensive. |
| Table 7 | Ongoing and interactive training on Phish or not Phish |
| Table 8 | Get rid of as many outward facing as possible. Go to the cloud!!! |
| Table 9 | Geo blocking and MFA |
| Table 10 | Geo blocking fo sho!! |
| Table 11 | Geoblocking…a must have. MFA has been the biggest factor to improvement. Possibly doing Phish testing. |
| Table 12 | Several items in the previous rankings. Geoblocking, LAPS for Windows device permissions, minimizing local admin access. Scan for PII existing in your collaborative space.  |
| Table 13 | Implementation of app locker on windows devices to prevent certain file types from being run. |
| Table 14 | Educating users has the biggest impact. Sending phishing emails from Microsoft that automatically assigns training when users click a phishing link.  |
| Table 15 | Removing local admin rights for users.  Require 2-factor anytime something is being done on a computer that requires admin rights – Cisco DUO (pricing based on per user of the tool).  Internal Vision Test or simulations.(“We turned off the internet to our district.”  A little humor from our table.) |
| Table 16 | Stopping PII sharing through email, SFTP and EFAX Solution.  WAZUH that allows you to pull multiple logins together to be more secure.   |
| Table 17 | Tabletop exercise with leadership team that would trickle down to staff- Did a brute force attack on all passwords of admins and showed in real time how quickly their passwords were stolen and discussion of how many other accounts were using those passwords. Also completed phishing exercises in district.  |
| Table 18 | PhishID, have an incident response plan in place if there were to be an issue such as a breach of accounts, Educating end users annually and throughout the year |
| Table 19 | Take away staff Admin computer rights |
| Table 20 | It’s a combination of efforts, from disabling account, phishing and client awareness tools.  |
| Table 21 | Fortinet - Security Awareness Training; it’s free, modules and participants get a certificate and it’s specific to K-12; Also, CISA scan.   |
| Table 22 | OpenCanary honeypot VM/SW; Self-serve password reset |
| Table 23 | People Side of Training - constant communication via email is important.  If someone has forwarding on their email, the CIO will receive a notification, then  reach out to them to have them remove forwarding from their email. |

Topic 4 - Internet Safety & Security Regulation–Updates & Modernization

**Q1 - Responsible Use:** Are you in favor of modernizing to responsible use policies in the formal KAR and KSBA model policy? **Why/Why not?**

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Yes - these need to be updated to fully encompass all our new technologies. |
| Table 2 | All yes, must be updated regularly - like model/guidelines at state level with ability for district boards to modify |
| Table 3 | Hard to answer without seeing it, the district uses their current AUP as backing behind discipline issues (staff and students).  Wouldn’t want this weakened to give the district less leverage. |
| Table 4 | All Yes-makes sense, you have to do this |
| Table 5 | Yes, their should be a up to date baseline model to maintained and matched to KAR and KSBA. Users are always changing, as well as an ever increasing in size. New risk show up with growth, so stating up to date  |
| Table 6 | Yes - emerging technologies are best addressed by responsible use rather than restrictive AUPs. RUP puts more onus on staff and students. |
| Table 7 | 7 Yes. We need fresh and updated guidance |
| Table 8 | Yes. Data security concerns need added. AI guidance needs added.  |
| Table 9 | Yes. Most districts adhere to the KSBA policies.  |
| Table 10 | Yes because it creates consistency and from a trusted source. |
| Table 11 | This aligns with other KDE initiatives like PBIS, but the current gap is that we all need to be at least at the CIPA level or better. |
| Table 12 | Yes. Today it’s probably better to frame this in terms of general expectations rather than trying to call out specific problematic activities as we’ve done in the past.  |
| Table 13 | Yes - The obvious thing to do…changing technology |
| Table 14 | Yes. Policy needs to reflect emerging technology. |
| Table 15 | Yes, since the way everyone educates across Kentucky is the student has a device right off the bat.  So if you don’t want that, the family needs to opt out.  And if KSBA does a model policy that all district would then follow there would be consistency across the state. |
| Table 16 | Yes.  As long as the districts have input into the RUP and that it meets the requirements of CIPA.  Would also be nice for district to be able to edit the doc to put their own spin on it. |
| Table 17 | Yes, because we typically use what they already have.  |
| Table 18 | Yes, policy needs to be up to date, KSBA is often the end-all-be-all   |
| Table 19 | All Yes.  More thinking is needed around the Opt-Out (and impact on things like eRate) |
| Table 20 | Yes, with a caveat for amendment for changing environments.needs. |
| Table 21 | Yes, want to know more about the “opt out” option. |
| Table 22 | Y: 6 N: 0  Like to have authoritative text to use; existing it clearly out of date  |
| Table 23 | Yes, you have to evergreen everything.  Social Media is already an Opt Out once per enrollment. |

**Q2 -  ​Formally adding an Opt Out model:** Historically, districts have operated in an opt in model (getting everyone to sign something every year), does it help your annual processes to explicitly offer an opt out model (restricting access for only the students who submit an opt out form) for your students?

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Not a fan of opt out |
| Table 2 | Yes, easier to administer. Some doing already. |
| Table 3 | As long as Rapid Identity provisioning solution can help to address this, it could work.    |
| Table 4 | Great idea, but might confuse parents. |
| Table 5 |  |
| Table 6 | Prefer opt in. Teachers would have to adapt instruction for those that have opted out.  |
| Table 7 | Yes, but how do we deal with Opt Out students and parents in terms of understanding the impact |
| Table 8 | Opt out is cleaner and really very few even do the opt out option. |
| Table 9 | Very few students opt-out. They do receive altered forms of instruction. |
| Table 10 | Yes and it works well through OLR |
| Table 11 | We've already implemented this in other areas, and online enrollment makes it easy. |
| Table 12 | Yes. Can quickly assign devices to many and establish accounts based on your enrollment rather than having to wait for form collection.  |
| Table 13 | Not an issue because it’s part of Online Registration. |
| Table 14 | OLR helps with this.  |
| Table 15 | Opt out is the way because today’s K-12 student is coming to the table with a device (provided by district), so make it an opt out. |
| Table 16 | Consensus yes.  Less districts have to track and manage.  What will be options for account usage if a parent opts their kids out?? |
| Table 17 | Yes easier than getting back every single year.  |
| Table 18 | Yes - saves time and opting out will make for hard times…just saying  |
| Table 19 | Yes, especially if they take away online registration |
| Table 20 | Yes, with consideration for how it will affect the student’s education. |
| Table 21 | No, unless they are still able to test, just not doing work digitally and would have to have packets.  Did we understand this question?   |
| Table 22 | All interested, see beneficial as long as lawyers/admin will support |
| Table 23 | Yes,  Social Media is already an Opt Out once per enrollment. |

**Q3 -** Providing for the safe, secure and responsible use (including ethical uses) of **emerging technologies** (such as artificial intelligence), - Are you in favor of including emerging technologies (such as AI) in your model policy from KSBA, as opposed to creating a completely separate AI policy?

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Yes - AI & Emerging Technologies to cover all bases. |
| Table 2 | Yes, emerging tech is so generic, not specifically AI. |
| Table 3 | If AI policy is *required* then merge them together, but keep it evergreen. |
| Table 4 | Combined |
| Table 5 |  |
| Table 6 | Yes, having a single policy is cleaner and more manageable. |
| Table 7 | One policy |
| Table 8 | Use general language to include the AI model guidance to allow districts room to create their own level of policy |
| Table 9 | Yes- Should be included as emerging technologies. As soon as it is labled and described as AI, potential change will require a new doc. |
| Table 10 | Yes. It will provide the broad guidelines which allows more specific processes/procedures at the local level. |
| Table 11 | Yes, and the reason is that we don't want to have such a narrow focus that it becomes outdated in a year. |
| Table 12 | YES. AI specifics can be placed in guidelines and the larger expectation can be set in AUP/RUP. |
| Table 13 | YES |
| Table 14 | Yes - one policy |
| Table 15 | All in one policy.  It would be a nightmare for teachers if there were multiple policies that were being kept track of. |
| Table 16 | Yes.  Because less is more and why create more work for yourself.   |
| Table 17 | Yes, because it ensures consistency and fits in the same bubble.  |
| Table 18 | Yes to one for all - if districts want to go above and beyond they can. |
| Table 19 | Yes.  These technologies are getting baked into everything so should be baked into the KSBA policy |
| Table 20 | Yes, with a baseline/guideline in place. |
| Table 21 | Yes |
| Table 22 | Include: 6 Separate: 0 ; one concern about guardians who might want to opt out of AI only |
| Table 23 | YES!  YES!  YES!  Everything we can do to have them all consolidated! |

**Q4 - Prohibiting Cell Phones** (and social media) **-** How will your teachers react to this?  Will your students understand it?

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | All on making sure the regulations and policies get regulated. |
| Table 2 | Already prohibited depending on the school. Getting around with smart watches. |
| Table 3 | Two districts already implemented, and it works great.  Others will need to make sure the teachers are all on the same page and enforcing the same way. |
| Table 4 | Some can’t because of accessibility, others are already starting to implement in certain schools |
| Table 5 | You can’t provide a tech solution for a people problem |
| Table 6 | Teachers generally OK with it for instruction, but not for their own personal access. Districts should be allowed to define what is/isn’t accessible and what is/isn’t social media. |
| Table 7 | Mixed response from teachers; and students will not want to follow the new rule. Chrome book is a work around to having phone! |
| Table 8 | We already say no to cell phones…but it's almost impossible to police. WIll make an undue burden on the classroom teacher. |
| Table 9 | Most districts at table 9 restrict cell phone use during instruction and some for the whole day.  |
| Table 10 | Teachers will be fine with cell phones. Students largely will not understand it |
| Table 11 | We're only addressing cell phone use as a disciplinary issue with this policy, not as a way to teach responsibility. |
| Table 12 | They’ll like it. Enforcement will be the challenge as some students may not give up a phone, etc. Consistent enforcement will be the key. |
| Table 13 | Teachers will want the school board to ban them.  How will it be policed will be biggest concern.  Students will be unhappy. |
| Table 14 | Teachers will be on board but will take some time.  |
| Table 15 | No more BYOD.  Couple stated that some schools are using “bags” to put cell phones in.  But prohibiting a device doesn’t necessarily need to be in the policy. |
| Table 16 | Mixed reviews on what teachers will like or dislike.  Feel like most teachers will probably be happy with no cell phones.   Feel like kids won’t understand. |
| Table 17 | Most teachers don’t allow it already. Some districts currently using cell phone lockers or storage pockets. Kids will be okay with it.  |
| Table 18 | Teachers will be fine, students will complain, parents will be the biggest issue if not allowed in schools |
| Table 19 | Teachers - They want it anywayStudents - More about the parents against it.  Students obviously would be unhappy |
| Table 20 | Teacher should love it as it reduces distractions within the classroom. |
| Table 21 | Teachers will like it.  Students will not understand and not like it. |
| Table 22 | Teachers: a couple think teachers would like; a couple not sure; a couple think opposed;  |
| Table 23 | No … Teachers are going to be frustrated and parents will have an issue with their child not having a cellphone.  |

**Q5 - District approved inspectable & traceable Electronic Communications Technologies (SB181)** - Beyond email, are you currently set up to have your schools ONLY use other approved inspectable & traceable digital communications tools?  If not, how big of a lift will this be for you?

|  |  |
| --- | --- |
| Table # | The ONE Big Idea |
| Table 1 | Nobody currently doing this and that it would be a HUGE lift to accomplish this task |
| Table 2 | Policy doesn’t prevent usage. State rule will help. Not huge lift. |
| Table 3 | It is a lift for coaches to use one approved app, but teachers got on board.  It addressed parent complaints of multiple apps. |
| Table 4 | District level Remind, another district through website hosting they can do groups |
| Table 5 | The Ban App. Always a heavy lift when getting teachers and staff to utilize any app that's new “required” to use. |
| Table 6 | Not ready for it. Many components used daily do not operate under the inspectable and traceable requirements (IC emails; LMS communications, etc.) |
| Table 7 | This is a challenge to control and need guidance and approved tools |
| Table 8 | This is too much of a lift to ask of a district to manage and stay on top of. We have official apps for communication available, but they are difficult to control. Unrealistic. |
| Table 9 | All forms of communication should be traceable.However- planning and restricting certain apps and websites will be challenging. Slippery slope to limit and restrict personal devices.  |
| Table 10 | Mostly not set up for this currently and a large budget concern to standardize tools across the district. |
| Table 11 | Not a lift, it is going to help. We have an approved communication tool already and it has helped immensely.  |
| Table 12 | Yes, currently set up for it. However, some rogue teachers/coaches may bypass the standards and use an unapproved tool. Some of the inspectable tools are fee-based, which creates another funding challenge and a solution to be monitored and managed. |
| Table 13 | Yes (Parent Square).  Sports teams folks haven’t been happy about using certain tools. Monitoring on some platforms isn’t possible….may become a major challenge.   |
| Table 14 | Not currently set up for district approved tools. Will be difficult to police until something negative happens due to someone using a non-approved tool. |
| Table 15 | We say it, but also know that people set up personal accounts to communicate to athletic teams.  DOJO is used and if it was taken away buildings would implode.  It was stated that districts are trying to fold communications into district “owned” methods. |
| Table 16 | These tools are being used in the district but not sure the district are not enforcing the monitoring of these programs.  Would be a big lift because someone has to the monitoring.  |
| Table 17 | District already have policies in place to use appropriate and designated communication tools. Won’t be a big lift and will help to have legislation to back up district’s standpoint on using specific approved communication tools.  |
| Table 18 | Not across the board - pockets of the same app/communication. As for the lift - if mandatory, it will be done, if optional - more difficult. |
| Table 19 | Yes and No.  Remind is used openly as well as coaching software.  It will cost the districts money as they will have to pay for a service to police |
| Table 20 | Yes and the lift isn't as heavy if this effort is reinforced by district leadership. |
| Table 21 | Yes, we are doing it, but can’t stop staff from using other tools that they can’t support. |
| Table 22 | Ready today: not at all; don’t even know what schools are usingBig lift: for most, yes, significant (coaches, band directors, etc.) |
| Table 23 | Yes, things are in place but not inspectable. |