ena@ Education Networks of America®

4 Cybersecurity Concerns for State Leaders

During SETDA's 2018 Emerging Technologies Leadership Forum (ET Forum), several state education technology leaders participated in a roundtable discussion that covered four key areas of cybersecurity:

- User vulnerabilities
- Network security
- Cloud and data security
- Student data privacy

Groups were given four sample scenarios to analyze and discuss. We have compiled their responses and feedback into a concise guide that we hope you find useful and valuable.

User Vulnerabilities

Fictional scenario: Email phishing

According to the superintendent, an employee who has access to all employee W-2 forms received an email request from a person impersonating the superintendent. The employee forwarded the tax information without realizing that the message was not being sent to the real superintendent.

Identified challenge:

Because policies are often made at the district-level, most state education departments lack visibility and cannot mandate that certain practices or procedures be put in place.

Recommendations:

- Encourage open dialogue, transparency, and honesty among all the state's school districts. Cyberattacks are becoming increasingly common and should not be viewed as a stigma; instead, schools should leverage their experiences to help their peers and inform best practices.
- Support the creation of school district peer groups within the state.
- Educate school districts to be more proactive when they see abnormal activities taking place.
- Develop and share a list of recommended training and education resources for school districts.

Network Security

Fictional scenario: DDoS attack

For the last three days at 2:00 p.m., the district's network has been going down. You are working with your ISP and are pretty sure a DDoS attack is happening because traffic is suddenly being sent to you from all over the Internet. You must spend time with your ISP each day to bring your network back up. Despite the team's efforts, the problem reoccurs. You assume a student or someone at one of your schools may be causing the attacks. Testing is coming up. How do you address the situation? What is the response?

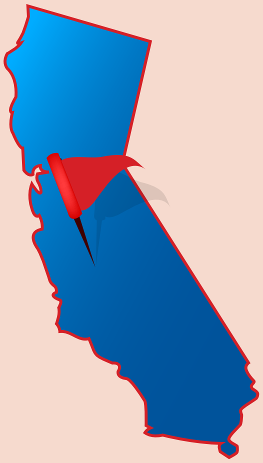
Identified challenge:

Some school districts, particularly smaller school districts, do not have a comprehensive action plan in place that addresses the various steps that need to occur when their district experiences a cybersecurity attack.

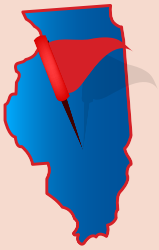
Recommendations:

- Engage Internet service providers before an attack occurs to discuss the school district's potential vulnerabilities and create a defense and mitigation strategy and action plan.
- Institute an action plan that identifies the processes and procedures that need to be implemented during a network security breach.
- Obtain resilient connections to maintain critical work flows and testing environments if an attack occurs.
- Educate community and board members on the importance of network security.
- Develop a comprehensive communication plan that includes a designated point person who is responsible for speaking with the media.

State Spotlights



California has a program called the Cybersecurity Education Program (CEP) that is designed to engender a culture of cybersecure, cyber-aware, and cyber-enabled workforce. The program provides every member of California's K–12 education system with a robust set of cybersecurity resources, assessments, and training modules at no cost.



Illinois is creating phishing tests and resources that school districts can utilize to help monitor how email is being used. The Illinois Department of Innovation and Technology developed an engaging security game to teach end users about the dangers of cybersecurity threats. Click here to take the quiz!

Cloud and Data Security

Fictional scenario: Ransomware

A teacher calls the help desk stating that there is a ransomware note on his screen. He was browsing his social media just prior to receiving the notice. At first, he thought it was an advertisement, but now he cannot get it to close. Two hours later, a second caller has reported similar issues with a ransomware note which prevents her from using the computer. The same message is displayed indicating files are now encrypted with directions for retrieving the decryption key. The user tells the IT team that the system showed infection shortly after opening up an invoice attachment. The message demands a bitcoin payment by the end of the week. At noon, a local news agency calls for comment on the story. At 1:30 p.m., the State Department of Education reports that multiple districts across the state have been affected.

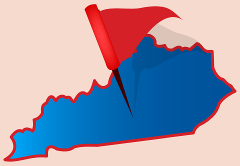
Identified challenge:

Most school systems are not required to create and maintain incident response plans.

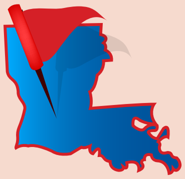
Recommendations:

- Educate your school districts on the dangers and probability of ransomware attacks taking place. School districts need to be equipped with the knowledge and tools to effectively address these attacks when they occur.
- Strongly endorse the creation and implementation of incident response plans.
- Explore various governing channels to create a mandate or mechanism that requires school districts to have an incident response plan in place.
- Encourage your school districts to run mock exercises and drills to ensure everyone is prepared in the event of a cybersecurity threat or attack.
- Speak with your peers to develop a keen understanding of what needs to be done from a technical aspect when an attack occurs.
  – Isolate the attack.
  – Prevent it from spreading.
  – Remove affected emails and exchange servers.

State Spotlights



Kentucky passed a state law that requires schools to have an incident response plan.



Louisiana instituted a law to ensure the privacy, security, and confidentiality of student data. Monetary penalties are enforced if a breach occurs due to improper practices. **Click here for more information**.

Student Data Privacy

Fictional scenario: Student data breach

Your state has partnered with a private company to deliver online state testing. The company manages the testing platform and all the associated data. You were just alerted that the company became aware of a breach that disclosed the information of over 150 students across the state and hundreds of student records from other states. Students affected attend several schools and are both middle and high school students. Data lost includes names, state ID numbers, grade levels, test results, teacher names, and possibly more. Your team has been assured that Social Security numbers are not shared with the company and would not be a possible addition to the list of data lost. District leaders, parents, and the media are regularly calling.

Identified challenge:

Maintaining student data privacy is critical in today's digital learning environments, but many education technology vendors are not taking the proper steps to comply with student data privacy policies.

Recommendations:

- Suggest schools work closely with vendors to make sure digital purchases comply with student data privacy policies.
- Incorporate student data policy reviews into the vetting process for digital asset purchases.
- Educate school districts on the importance of creating an action plan that addresses student data privacy breaches.
- Develop an education plan for teachers and staff on the importance of protecting student data privacy and the potential consequences that can stem from a breach.
- Encourage school districts to develop a system of governance based on their state laws that focuses on clear communications and addresses policies, processes, and best practices.
- Develop a comprehensive communication plan that includes a designated point person who is responsible for speaking with district leaders, parents, and the media.

ena@ Education Networks of America®

CONTACT US TODAY!

For more information about ENA, contact Lillian Kellogg, Senior Vice President, Client Services, at **(615) 312-6072** or **lkellogg@ena.com**, or visit our website at **www.ena.com**.

ABOUT ENA

Education Networks of America (ENA) delivers transformative technology solutions supported by exceptional customer care to education and library institutions across the nation. Since 1996, we have worked with our customers to design and engineer high-capacity and future-ready broadband, Wi-Fi/LAN, communication, cloud, security, and software solutions. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.