What you should know about the K-12 Cybersecurity Act of 2021

October 12, 2021

On October 8, 2021, President Biden signed the bipartisan K-12 Cybersecurity Act of 2021 into law. While the act offers little in the way of concrete reform, it represents both an important first step into the K-12 cyber landscape and a glimmer of hope that the federal government will be able to assist in both preventing and mitigating K-12 cyber incidents.

In noting (if understating) the breadth of information that schools maintain on students and employees alike, the act gives the Director of the Cybersecurity and Infrastructure Security Agency (CISA) 120 days to study the specific risks impacting K-12 institutions and, following that, 60 more days to issue recommendations for cybersecurity guidelines that schools can implement. In addition, CISA will be developing an online training toolkit for schools to educate officials about CISA's recommendations and to provide strategies for officials to implement said recommendations.

The act, of course, comes on the heels of yet another year of major cyber incidents impacting K-12 schools. According to the K-12 Cybersecurity Resource Center, there were more than 400 publicly-disclosed school incidents in 2020 alone – and that number is likely much higher due to the uneven reporting requirements that schools and districts operate within.[1] While 2020 undoubtedly added stressors to school and district IT resources, there is little to suggest that such stressors will recede anytime soon. As a result, districts would do well to keep a close eye on CISA's recommendations – even if they are presented as voluntary guidelines. This remains particularly true as cyber incidents are growing increasingly common, complex and costly.

For now, while it is tempting to say that there is nothing for districts to do while CISA develops its report, nothing could be further from the truth. In fact, much of what CISA reports is likely not going to be news to those who have been managing IT for districts over the past decade, if not longer. To that end, while CISA will, without doubt, highlight the vastly limited resources that districts

report being able to put toward cyber readiness, there are a number of steps districts should be taking now:

- Create a cyber-informed culture by ensuring staff and students are trained on best practices
- Prioritize endpoint (desktops, laptops, tablets, etc.) security
- Ensure network permissions (separating the student network from the faculty/staff network) are current
- Update (or develop) your incident response plan that can help bring the necessary stakeholders together

On this last point, thoughtful and thorough incident response plans are proving more and more critical to managing a cyber incident. Having a proper plan – and following it – can streamline a number of steps during the fog of an incident, from who to contact, what to say and how to step through the ensuing legal obligations.

---

[1] Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Available online at: https://k12cybersecure.com/year-in-review/

Authors

Jeff Knight

Of Counsel

Columbus
614.227.2346
jknight@bricker.com