Closing in on Cybersecurity Stability

Finding balance among safety, continuity and enablement of education is the real goal of K-12 IT these days, and that's not something you can buy in a box. Here's how to achieve it.

Fadi Fadhil
Cybersecurity Strategist
Palo Alto Networks

I GROUP THE BIG CHANGES IN K-12 THAT ARRIVED with 2020 into four elements:

1. Remote and hybrid learning is here to stay.

Now that teachers, students and families have tried salt in their food, they're not going to go back to the way it used to taste. Technology is here to stay. We no longer have to wonder whether the computer will replace the pencil, like we did with the onset of online high-stakes testing years ago. In three months, teachers transformed their instructional practices, making laptops the new classroom.

2. Software services have exploded.

The ease and simplicity of licensing and adopting software-as-a-service means schools have adopted learning systems that help with any number of activities – assigning and accepting homework, helping students practice specific skills, allowing for real-time engagement and collaboration, delivering content and the rest of it. However, now that means data – and especially personally identifiable information – is flying around, data that needs to be secured, monitored and prevented from being shared.

3. Issues of digital equity have become part of public discourse.

The technology have-and-have-not issue has existed seemingly forever. Prior to 2020, some schools did have one-to-one programs for computers and did leverage technology, allowing students to learn from anywhere, including from home. Often, the internet that came along with that was a low-cost, highly throttled deal that, when everybody had to stay home, hasn't held up well under the entire family's internet needs.

4. Bad actors have shown up to the party.

These sharks have smelled blood, which means we need to pay attention. While attacks began targeting K-12 in about 2016 in a serious way, those began escalating in 2018 and 2019, and by 2020 they skyrocketed. Like the pervasive use of technology in schools, cyber criminals are not going to stop or go back into their hiding places.

Traditionally, for good reasons, the conversation in K-12 has been focused on education. The priority for spending has been steered toward academics – getting more support and training for teachers and trying to control the classroom size, for example. Technology, and especially cybersecurity, was a scheduled expense, up there with predictable plumbing problems and textbook replacement, but contained within the IT organization.

However, IT – and especially cybersecurity – has now become a strategic element for education. Parents, superintendents, board members and executives within administration have realized that keeping data and systems safe can have a district-wide impact. Experience a data breach or a ransomware event and you'll suffer damages that strike your budget as well as your reputation: Families will leave your schools to go to the district next door that didn't have a break-in. That means it has become something that should be part of all decision-making.

Finding Your Balance

Unlike corporate America, K-12 can't sink a ton of money into cybersecurity and call it a day. There's hardly ever enough staff. Few districts can afford a dedicated chief information security officer. Funding new solutions can usually only happen one tool at a time. That means it's all about balance.

Picture a three-legged stool:

- One leg represents the ***safety*** of education, making sure people can use the systems and software without allowing the bad actors in.
- Another leg represents the ***continuity*** of education,

making sure that whatever happens doesn't shut down the district unexpectedly.

- The third leg is ***enablement*** of education, embracing the digital wave and taming it to work for your schools.

There is no silver bullet-in-a-box that you can buy to achieve this balance. But there is one step you can take that will help you move closer to stability. That's to leverage the industry and have conversations with experts. They'll help you elicit your district's specific strengths and weaknesses. Are your security and system tools configured properly? Do you know what your staff is good at and what expertise they have? What's the makeup of your district user base? Are they using school devices or their own? The answers to all of those kinds of questions should change the advice you get.

For example, in my new role at Palo Alto Networks, when a district person comes to me and says, "I need to figure out this ransomware stuff," I don't say, "Here, you need to get this firewall" or "You need to get this DNS solution." I prefer to ask, "Do you have a good handle on your devices? Do you have good governance in your district?" and so on. We talk. And then based on their responses, I'll recommend a particular approach. And I'll help them plan their next two or three steps. After all, cybersecurity isn't a one-and-done project; it's a journey.

I like to say, "Tools before strategy? You're headed for tragedy." If your vendors spend more time telling you how great their solutions are, reconsider whom you're listening to. Work with a company that can ask you critical questions that will help uncover what your situation really is in the bigger context.

The hard part is finding somebody who understands K-12 inside and out, to help you keep your balance on that three-legged stool, while also providing solid guidance based on true expertise. That's why Palo Alto Networks is investing in strategists like me who have a background in K-12. We know what you're experiencing because we've done it ourselves. That's what makes us different.

Reach out to Fadi via email *at* **fafadhil@paloaltonetworks.com** *to continue the conversation.*

Fadi Fadhil *is a cybersecurity strategist with Palo Alto Networks. Previously, he served almost 16 years in IT roles in K-12, including as CIO of Minneapolis Public Schools and Saint Paul Public Schools, as well as CIO of the City of Minneapolis.*