Cybersecurity: Q&A with PEPPM

1. What is cybersecurity?

It's a continuously developing discipline within the information technology (IT) arena. No one person can cover all of IT these days. The needs are too specialized. Cybersecurity narrows our focus and skill sets to the science and controls needed to keep you, your computers, data, networks, and electronic devices safe. From what? From school shutdowns, ransoms, denial-of-service attacks, money and data theft, lawsuits, employee grievances, bullying, embarrassment, and just plain-old mischief.

2. What are some of the emerging innovations in technology that will impact cybersecurity?

Everybody is familiar with antivirus software and firewalls. But they aren't perfect, and they can't work when users fall for social engineering tricks. Therefore, much of the current research, development and deployment for innovative products centers on threat detection, threat hunting and threat monitoring.

The challenge today is that bad actors – some backed by foreign governments – are patient and coy. Sometimes they will slip in a tiny one-line piece of code into an organization's system, then wait, wait, wait to build upon the learnings culled from that Trojan horse. We call this months-long intrusion process lateral movement. Over time, hackers stealthily obtain increased privileges until they deem the time is right to strike, whether drip by drip or sudden outright ransom demands. This pattern represents malicious innovation on the black-hat side of IT, which requires innovative offensive and defensive tools on our side.

3. How can technologies be used to eliminate the threat of cyberattacks?

Because of the human factor, no organization will be 100% safe over all systems, all users and all data, so we can't use the word "eliminate." But we can get close. We need those old-fashioned tools along with innovative cloud-based, real-time detection tools and hunting software. The current challenge is how to integrate all the old-school tools and software for ease of use and widespread deployment. The problem facing many school districts is that prevention technology is in different boxes (computers or servers) – for example, one defensive box for email and another for website applications. They need to talk to each other. They need to be less expensive. And they need to be easy for even a small school district to deploy or access. On top of that, our monitoring software must provide full coverage across all of our networks and infrastructure.

4. Why is cybersecurity evolving in education, and what can schools do to keep up?

Our tools and tactics evolve because, unfortunately, we are usually one step behind the hackers who are motivated by greed, power and ego. Their full-time job is to find vulnerabilities. To keep up, school boards need policies and strategies that prioritize cybersecurity. That means funding an adequate budget and prioritizing continuing professional development for IT staff. Districts should not be afraid to tap the expertise of consultants and leading-edge technology companies as well as free services and resources available to schools (i.e., Multi-State Information Sharing & Analysis Center, Cybersecurity and Infrastructure Security Agency).

Eventually, your staff will come back with recommendations, and many of the products and solutions will be instantly eligible for purchase and bid protection under a PEPPM purchasing contract. That means no delay in implementation.

5. What is one of the most effective ways to boost cybersecurity in education, and how can schools protect against increasingly sophisticated and malicious malware, ransomware and social engineering attacks?

Phishing schemes are responsible for 90% of intrusions and breaches, which, in turn, lead to ransom demands. We need to prevent human mistakes. An effective way to avoid attacks is to implement an ongoing immersive education strategy that trains employees and computer users to avoid social engineering traps. A good education strategy does not simply repeat the same "do-not-do-this" message over and over. Instead, constant phishing tests directed at users along with education to reinforce and cement in the learning is necessary. There are many network security awareness trainings available to help with this education process. **B**