Executive **Q&A**

Mission-Critical Status:

Foster a Strategic Mindset Around Cybersecurity

As campuses consolidate cybersecurity tools, they've finally elevated cybersecurity to mission-critical status. Palo Alto Networks' Darren Estridge says IT leaders must ensure strategic planning maintains a culture of cyber-awareness.

PRODUCED BY:

CAMPUS TECHNOLOGY

SPONSORED BY:

carahsoft

paloalto NETWORKS

FIVE YEARS AFTER COLLEGES AND UNIVERSITIES FIRST embarked on their great pandemic journeys—enabling the massive technology shifts required to meet students, faculty and other university employees where they work—campuses face new demands to support multi-cloud environments and artificial intelligence use cases and research. Locking it all down and protecting data and networks from on-premises infrastructure out to the edge requires new strategic thinking and planning.

Campus Technology recently spoke with **Darren Estridge**, VP of sales, SLED at Palo Alto Networks, about cybersecurity issues higher education must navigate today, and why consolidating cybersecurity tools may ease administrative burdens on time-strapped teams.

Q: What are some of the more dynamic changes you've witnessed over the last year or so on campuses?

A: COVID changed the way people work, learn and live, and some of what's happened over the past year is kind of an unwinding of some of that. People are coming back into the office, going back to campuses full time, but at the same time, we see a lot of universities spreading their wings. This was a catalyst for them to make changes in their own organizations and the way they go to market. Many have satellite campuses that didn't exist prior to COVID. They're buying universities in other countries, for distance learning or study abroad. As the environment that requires protection ebbs and flows, security requirements are exacerbated.

Q: The ways in which higher education approaches computing have evolved, but threats are evolving as well. What shifts have you seen from a threat perspective?

A: The biggest evolution is the introduction of AI into the threat vector. When you think about the threats universities face as they're being attacked by AI, there is no way that human intervention can prevent an attack; there's no way to keep up. We now must attack AI with AI.

Q: Higher education is also relying on a lot more OT and IoT technologies today. How has that affected the threat landscape and how campuses approach cybersecurity?

> **Universities' attack surfaces are very broad: It's not just on campus, it's wherever students go or wherever the administration happens to take a system or log into their tools.**

A: Universities' attack surfaces are very broad: It's not just on campus, it's wherever students go or wherever the administration happens to take a system or log into their tools. Every endpoint is a potential entry point, and a lot of folks have not fully appreciated that. For some time we've had cameras on campuses, endpoints and sensors all over the place, and each one is an opportunity for a breach, so having an IoT-type solution that can really protect those edge devices is critical. The breadth of risk is high. The more technology we implement, the more we need to protect.

Q: How can higher-ed leaders go about elevating cybersecurity to a mission-critical status?

A: It's something they've had a tendency to overlook. It's allowed unintended risks. I had a roundtable discussion recently with a very large state university, with the CIO and their staff, and the CIO said, "We really are an open campus, and we have to make sure we allow all of the users,

> **The AI sprawl and the advent of AI being integrated into everything that we do is something we need to stay in front of. Continual innovation and investment in research and development will be required.**

all of the departments to make their own decisions when it comes to technology. It's hard for us to enforce certain policies because they bring in the money. They have a budget and get to spend how they want."

I thought about that and asked, "Are you allowing them to choose their electricity and their water providers?" Of course, they don't. Unless you think about cybersecurity as mission-critical, as a requirement of the critical infrastructure you support, you're not going to have the control you need. If you allow them to make point decisions and buy point solutions without seeing how it fits into the organization's cohesive security strategy, you're undermining your own efforts.

Colleges and universities need to implement policies in which they secure all of these things while still being open. Some things will be required in order to use university resources. It's a bit of a dichotomy in higher ed because these institutions want to be open, and they need to be open, to have that freedom of thought, and exploration and innovation. But, certain guardrails are required so that they don't put a university at risk.

Q: We've seen data and AI sprawl as well. What's going to help them contain and protect that, to get a handle on all of that?

A: Whether it's cloud, or on-premises data protection, they need to take it seriously and implement policies. Many universities for many years have just allowed researchers to swipe a credit card to spin up a cloud instance and do whatever they want. They've often believed that because it's in the cloud, it must be safe. But if they read their agreements, they'll find that providers are responsible for protecting the cloud, not the data in the cloud. It's important to have a solution that protects data whenever they push anything to the cloud. Know that it's protected before it leaves and it's encrypted so that they can properly manage it throughout the entire lifecycle.

The AI sprawl and the advent of AI being integrated into everything that we do is something we need to stay in front of. Continual innovation and investment in research and development will be required. Universities can't do it by themselves; they need good partners. Buying point solutions to solve a specific problem without looking at how it integrates into the broader security strategy just ends up driving more sprawl. It's expensive to write a purchase order in the public sector. A lot that goes into it. Every single one of those purchases is governed by a contract vehicle, so there's contract management and compliance that goes along with that. If you can consolidate the list of vendors from 50 or 60 down to 10 or 15, how much more efficient and effective would that make an organization? How much overlap of the existing tools could you potentially have with 50 or 60 different point solutions in your environment? Consolidating and constructing a strategy with fewer vendors, fewer relationships to manage and fewer contracts to own, ultimately saves money.

Palo Alto Networks employs close to 400 people who wake up every day and only think about state, local and education. Our goal is to give our customers the confidence they need to trust us with their most important technology assets. Learn more about Palo Alto Networks's work in higher education, at https://www.paloaltonetworks.com/industry/public-sector.