KEY TAKEAWAYS

The Growing International Cyber Threat Facing Research Universities

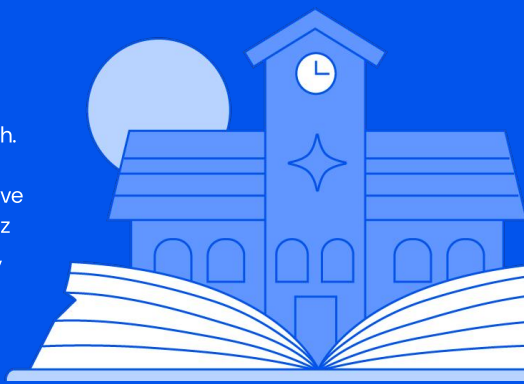
THE CHRONICLE OF HIGHER EDUCATION

WITH SUPPORT FROM WIZ

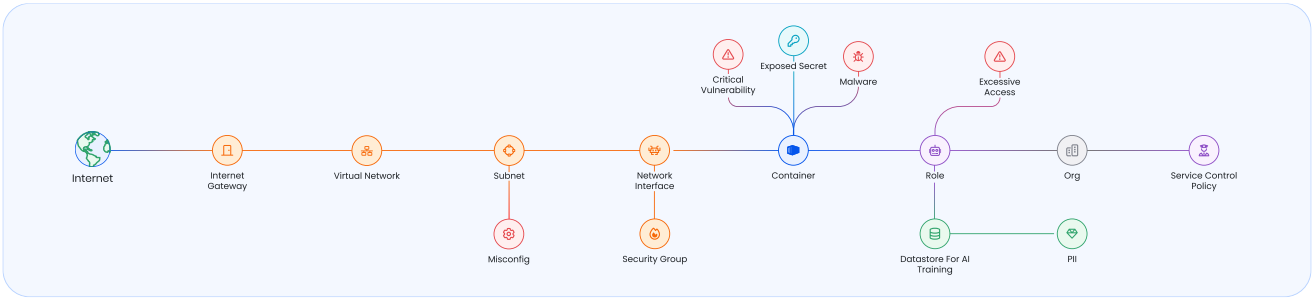
Wiz for Education

Helping education focus on learning, not cloud risk

Cloud and AI are becoming core to how education institutions teach, operate, and conduct research. As adoption grows, understanding what's deployed, how resources connect, and who has access becomes critical. Wiz prioritizes risk with context and guides remediation, helping lean IT teams move from basic visibility to confident action. By democratizing security insights across departments, Wiz empowers researchers and administrators to share responsibility for their own cloud environments, freeing them to focus on their institution's teaching, research, and innovation efforts.



Wiz helps educational institutions quickly understand and reduce cloud risk by giving IT and security teams a clear, contextual view of their environments. Built-in data discovery and classification show where sensitive student and research data lives and how it is exposed, supporting requirements from FERPA, CIPA, and GDPR across cloud resources.



Comprehensive cloud visibility with context-driven risk prioritization

Wiz gives education institutions clear visibility across their cloud environments through an agentless, API-based integration. By quickly identifying cloud resources, network connections, and identity access permissions, Wiz shows how systems interact and where real risk exists, helping teams focus on what matters most.

Accelerate secure AI adoption with continuous insight into AI workloads and resources

Wiz gives teams a clear view of AI services, models, data pipelines, and cloud resources, including managed GenAI platforms, custom trained models, and research workloads. This helps identify Shadow AI, misconfigurations, and exposed resources and sensitive student and faculty PII data in minutes, not days or weeks.

Help teams secure the software lifecycle from code to runtime

Wiz secures the software lifecycle by connecting code findings, cloud configuration, and runtime behavior into a continuous security workflow. This gives researchers, IT, and SOC teams a clear, end to end view of risk, helping them identify root causes and remediate issues earlier with less operational overhead.

> Many people see security offices as places where good ideas go to die, but the reality is that if we work together to use our cloud effectively, we can work faster and safer with cybersecurity built in from step one.
>
> **Director of Cloud Security, Private Research University**

The Growing International Cyber Threat Facing Research Universities

Key Takeaways From a Virtual Forum
Presented by *The Chronicle* and Wiz

HOST

Ian Wilhelm
Deputy Managing Editor,
The Chronicle of Higher Education

SPEAKERS

Anita Nikolich
Director of Research and Technology Innovation and Research Scientist, University of Illinois at Urbana-Champaign, School of Information Sciences

Joseph Nwankpa
Director of Cybersecurity and Associate Professor, Information Systems and Analytics, Farmer School of Business, Miami University

Eric Zematis
Chief Information Security Officer, Lehigh University

The strengths of America's research universities, such as their intellectual-property and open-research collaborations, also make them vulnerable. In addition to ransomware and phishing scams, America's pre-eminent institutions face increasing espionage and intellectual-property theft by countries competing with the United States.

How can research universities protect themselves from these emerging threats? What should institutions look out for as cybercrimes become more advanced?

To learn more about this issue and explore potential solutions, *The Chronicle* held a virtual forum on January 22.

The following comments, edited for clarity and length, represent key takeaways from the forum. To hear the full discussion, watch the recorded webinar here.

Ian Wilhelm: Can you give us a sense of how to think about what I broadly describe as an international cybersecurity threat?

"Part of what we see are more state actors that are going for the kind of long-running, persistent access to universities. This is pretty new."

Joseph Nwankpa: The universities are facing an enormous threat. Part of that is driven by how our society and the economy have become a digital landscape. That has really exacerbated the type of threat that we face today. Part of the challenge that we face is the university is designed to be a collaborative institution. At the university, one of the things that we do is try to disseminate knowledge, trying to build that network. Now we have a significant amount of threat actors, especially state-sponsored threat actors, that are trying to find a way to gain advantage, to be able to tap into research and development, tap into innovation, tap into the next new thing.

Anita Nikolich: Targeting academia fits this broader pattern of targeting critical infrastructure. Part of what we see are more state actors that are going for the kind of long-running, persistent access to universities. This is pretty new. In general, countries that are very skilled at this are China, Iran, Russia, and North Korea, and they have years

of experience in advanced persistent threats and getting into university systems. We're just seeing this mimicking the pattern of volt typhoons, salt typhoons, of low and slow, persistent entry into places where they can gain a foothold to do other things — perhaps without us even knowing — for many, many years.

"When you're dealing with the more sophisticated actors, Lehigh or Miami University or the University of Illinois really doesn't compete with China. It's asymmetric."

Eric Zematis: The vast majority of attacks against universities are international — you don't want to be a domestic attacker of a university, because the FBI is going to show up at your house. That international threat is in two categories. One is organized crime, and the other is the nation-state actors. What they're looking for is very different. Typically, the threats that are the organized-crime type are collaborations with various groups that are designed to quickly take funds through ransomware, or through sextortion, or through misdirection of funds, or misdirection of payroll. We typically will see an attack and then a direct target, and the attempt to leverage that kind of attack very quickly.

The more disturbing things are where we see some evidence of an attack with no clear objective. Those are often those low-and-slow nation-state actors that you don't know what they're looking for exactly. You know they targeted people in your research community, but they didn't try to misdirect their payroll, or any of those things. So you have conversations with these groups: Is there anything you're working on that is particularly sensitive? And usually the answer is no, I'm all fundamental research — but that doesn't mean that it's not targeted, either for disruption, or to try to steal that intellectual property.

One's like a smash and grab — you're just gonna bust in and grab the cash register and run out — and the other one is more like sophisticated art thieves that are doing the Mission Impossible-style intrusion. We can very easily have prevention for the smash-and-grab types, but when you're dealing with the more sophisticated actors, Lehigh or Miami University or the University of Illinois really doesn't compete with China. It's asymmetric.

Wilhelm: I'm curious about where we've gotten to when it comes to building a culture of security within the researchers on your campus? How do you think about that balance between being open to collaboration and dissemination of knowledge and the idea that, hey, this stuff has to be secure, and we've got more actors out there who want access to it?

Nwankpa: That's one of the things that we continue to grapple with. Let's say that I'm working on a project, and information about the economic situation in China would be critical. It makes sense for me to collaborate with a Chinese researcher — the problem is that more often than not, I don't have any way to validate that somebody that I meet at a conference is a legitimate Chinese researcher. All I see are footprints on the internet.

It's difficult for researchers to take a step back and think, hey, maybe this might be a concern, because we are really wired to push that research agenda. There's a lot of pressure in R1 institutions to publish top-notch research. If we could find a way to be able to do an appropriate validation, that's going to put us in a great position. But right now, it's just so difficult, because the goals are not aligned. On the one hand, the researcher wants to do research and be very productive. On the other hand, they have to also take precautionary measures to mitigate this threat. Sometimes that's just too much to ask.

Nikolich: Universities increasingly host larger, more complex, very expensive research infrastructure, whether it's microscopes or computers or things like that. The challenge is that this is often distinct from university central IT. This is a problem. There's not funding specifically around security.

What we've tried to do is say, let's look at this from a risk-management perspective. That's something that's more in the forefront, not only in the minds of people who run infrastructure, but also the funding agencies are starting to think about this, to be a little more prescriptive about thinking about it. In the past, you didn't have to have any security around this very expensive research infrastructure. Now you really do need two-factor authentication and things like this. So slowly, I'm seeing that yes, there's openness for the research, but protecting the stuff on which we do the research — people are starting to realize that that's equally important.

Zematis: The research community at a university is a couple hundred or a couple thousand — depending on the institution size — entrepreneurs. They have a problem they're trying to solve, and they have to be laser-focused on that problem. Often there's a problem

of visibility. It just doesn't even occur to them to bring in partners on campus to help them manage security, to understand the risks.

The most valuable approach is building a culture around ownership of security. If we can help the principal investigators and other research communities on campus feel like security's a problem that they need to address, then my team and I can be brought in. If I'm an obstacle, they're just going to go around me, or over me, or through me. One thing I've learned in my decades of tenure in higher ed is that I don't want to have to be smarter than the researchers on campus, because it's a game I can't win. I need to think about how I can provide value to them, so that they're going to come to me for support, rather than me trying to find out everything that everyone's trying to do.

Wilhelm: What kind of training works for researchers?

Zematis: I'm not a big believer in generic training, because, as I said, we have 500 different entrepreneurs on campus that all have a different focus. We do have some generic resources we could point people to, particularly people who are working in health research. There might be HIPAA resources and those types of things that we guide them toward. But it really is about trying to tailor something to their individual needs, so they understand, what are my responsibilities, what's automatically being handled? One of the advantages of Lehigh being a medium-sized institution is that we have the ability to be more bespoke and custom.

"The most valuable approach is building a culture around ownership of security."

Wilhelm: How are you thinking about artificial intelligence when it comes to the threat assessment for your campus? How AI may be used by bad actors, but also how it provides some defenses?

Nwankpa: The challenge with AI is that it does increase your attack surface. But on the other hand, we do see an upside with AI when you look at things like threat detection, outlier detection, being able to leverage AI to be able to identify patterns.

Nikolich: I'll take a little flip side of that. I've been in and around AI security for almost six years now. The biggest threat I see are these agents and agentic AI on campuses, because the No.1 threat from that is privilege escalation and access-control violations. That threat surface is going to become a university threat surface really soon.

Zematis: AI lowers their cost of operating. If I cut in half my cost of doing an attack, it means I can do twice as many attacks for the same cost. These people are looking for return on investment. That really does increase the number and frequency of attacks. We've seen an explosion in phishing attacks and other types. So we need to respond in kind with other versions of AI, which, of course, raises our costs, right? As their costs lower, our costs have to rise.

This Key Takeaways was produced by Chronicle Intelligence.
Please contact CI@chronicle.com with questions or comments.