KEY TAKEAWAYS

The Rise of the CISO in Higher Ed

WITH SUPPORT FROM hp

THE CHRONICLE OF HIGHER EDUCATION®

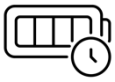
Are you ready to empower your institution with the World's Most Secure PC[1] solutions?

Industry's First Self-Healing BIOS

HP Commercial PCs safeguard your students' data with our unique Sure Start[2] technology. This self-healing BIOS ensures firmware and BIOS integrity, crucial in government settings. It's aligned with NIST Guideline 800-193, offering top-tier security compliance for government institutions.

Product Lifecycles and Transitions

Upon standardization of an HP Business product, we can notify you of the discontinuation date of the product (barring any unforeseen industry-wide events that are outside of our direct control). HP is focused on smooth lifecycle management. We conduct regular meetings to discuss product roadmaps, product lifecycle transitions, upcoming projects, best practices, etc. HP typically plans for 3-6 months of overlap between legacy and replacement platforms through custom communication sent to your administrator.



HP Long Life Battery Warranty

The HP Long Life Battery, matched with a 3-year warranty, offers substantial savings and environmental benefits. This aligns with the budgetary and sustainability goals of Higher Education institutes minimizing user disruptions due to replacements and supporting eco-friendly practices.

PC Pricing

Understanding the budget constraints of educational institutions, HP ensures competitive, sustainable, and predictable PC pricing. We offer consistent pricing for your institute's PC standards, making long-term financial planning easier. HP can offer a "like for like" PC transition commitment for the next generation of product standards (provided the platform and configuration is close as possible to the original and that HP's component costs do not increase).

Resource Alignment

Ensure your vendor of choice is investing and aligning the right resources to support the needs, requirements, and responsiveness of your institution. HP can provide details on these resources and investments aligned directly to your account.

Sustainability

The fastest way to achieve your institute's sustainability goals, is to ensure that they buy from and partner with a sustainable company. HP continues to set bold, long-term goals and focus strategies where it can have the greatest impact – this includes design, deliver, and recover our products and solutions. Our goal is to reduce the number of materials in products, increase use of recycled content, design for energy efficiency, and offering convenient and more sustainable services.

Manageability

HP equips Higher Education Institutions with modern lifecycle management solutions that deliver protection, visibility, and control for PC's.

HP invites you to connect with our education sales representatives to set up a workshop to assess your institution's specific printing servicing and usage requirements.

Sources

1. Based on HP's unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs and HP Workstations with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

2. HP Sure Start is available on HP Commercial PCs only.

The Rise of the CISO in Higher Ed

Key Takeaways From a Virtual Forum
Presented by *The Chronicle of Higher Education* with support from HP

MODERATOR

Ian Wilhelm
Deputy Managing Editor, *The Chronicle of Higher Education*

SPEAKERS

Kim Milford
Deputy Chief Information Officer and Chief Information Security Officer, University of Illinois at Urbana-Champaign

Blake Penn
Chief Information Security Officer, Colgate University

Andrea Simpson
Chief Information Security Officer, Howard University

As cyber threats to higher education grow, so do efforts to prevent them. Colleges are bolstering defenses, educating their campus communities about the threats, and in many cases creating the role of chief information security officer, or CISO. What does a CISO do? How is the role different for higher education compared to other sectors? How can the role improve cyber security?

On February 8, *The Chronicle*, with support from HP, convened a virtual forum, "The Rise of the CISO in Higher Education," to discuss those issues. The following comments, which have been edited for clarity and length, represent key takeaways from the forum. To hear the full discussion, watch the recorded webinar here.

Ian Wilhelm: How has the role of CISO evolved over time?

Kim Milford: When I started, in the early 2000s, I had to understand how the technology worked. I had to find the right vendors and partners to work with me to solve our needs. We all had small teams back then. It was very network focused. I knew networks pretty well, so I could really apply myself there. We talked about proactive controls, antivirus sorts of things. Twenty years later, institutions have outsourced quite a bit, so there are lots of ways you can do security. Now I have to look across a fairly big picture and a fairly big team.

Wilhelm: How much of your time is spent as a college leader versus technologist?

Blake Penn: I don't really spend any of my time with technology. We have people who do that whose job titles have technical stuff in them. I used to be very technical, but my job now is to understand what they're talking about. I need to know the language, but I don't need to know the details. I just have to make sure that we're on the same page with what we're talking about. If something gets a little too technical, beyond where I am nowadays, I'll just ask them, and given my background, I pretty much pick up on stuff. It's a very political job. It involves a lot of emails, meetings, and compromise.

"Being in this seat of CISO is really all about managing risk and not necessarily about the technology or the tool sets. You're trying to protect the university, so how are you going to do that?"

Andrea Simpson: Being in this seat of CISO is really all about managing risk and not necessarily about the technology or the tool sets. You're trying to protect the university, so how are you going to do that? If you can't protect it, what's the risk? If you don't protect it, what is exposed?

Milford: As a CISO friend of mine told me, "I'm not a technologist, but I have to have a technology B.S. radar." I have to know the technology well enough to know if it is the right solution and if we are applying it right. This job is more strategic than technical. My staff don't need me in their lane mucking everything up. They trust me for higher-level strategic outreach and helping my CIO understand things better so that she can make better decisions.

Wilhelm: Who do you report to at your university?

Penn: I report to the chief information officer. I would say that's pretty typical in higher education. When I did consulting, I got to see a lot of different industries and how they work. I noticed a change over time from the default that the CISO would report to the CIO, particularly in highly regulated industries like finance, where they're reporting to some chief risk officer through legal and compliance. I think that makes a lot of sense too.

Milford: I report to the CIO and the reason traditionally I think we started with that was because we have this technology knowledge and it was hard to explain. It was hard to jump the bridge into the business leaders and explain what we need to do, and the CIO could help us with that. I've seen successful models of the CISO reporting to the CIO, the chief operating officer, or to the board. It really depends on the culture of the institution and the structure and policy of the institution.

Wilhelm: How are you thinking about generative AI and other similar tools?

Simpson: You have to have good, clean, clear data in place. AI is only going to give you whatever you train it on. Our focus right now is really cleaning up those data sets and getting an understanding of what data is important to the university, especially when it comes to the students. We put out a general policy to say that you cannot use and upload data from within the university to any AI technology that's not already approved. On the technology side, we blocked certain things so you can't get to it. We have alerts in place to stop people from pulling data and uploading it to ChatGPT.

"The thing about AI is that this is really nothing new. It doesn't bring up new challenges as much as it creates a variation on the old ones."

Penn: The thing about AI is that this is really nothing new. It doesn't bring up new challenges as much as it creates a variation on the old ones. If you're talking about protecting student data, we do the same things with AI that we do with anything else. We fundamentally want to protect security and privacy. We identify risks and then put controls in place to get the risks down to an acceptable level. One of the big things I think it did unearth was the sharing of institutional data with third parties. If you put institutional data into ChatGPT, they now have it.

Wilhelm: How do you better manage risk in research?

Simpson: It's more about education for the research community. "Hey, yes you're doing research, but you're doing research on behalf of the university, so it's really not yours, it's the university's." We have to get them to understand that we're protecting all of it. They need to follow the rules, make sure we have backups, make sure they are encrypting it. Make sure they are doing everything they can to ensure that the work they are doing can continue.

Wilhelm: What does it take to be a good CISO?

Penn: You have to have ice water in your veins. You have to be levelheaded in any sort of crisis. If you're risk-averse, if you're susceptible to stress, it'll drive you crazy. You're occasionally going to have big breaches and things you don't like. You still must engage your intellect and rationality and reasoning skills that you've learned over your career to make sure that you're effective and can successfully navigate this water.

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

THE CHRONICLE OF HIGHER EDUCATION®