CASE STUDY

Managing a Changing Threat

Colleges rethink the role of the information security officer amid online breaches

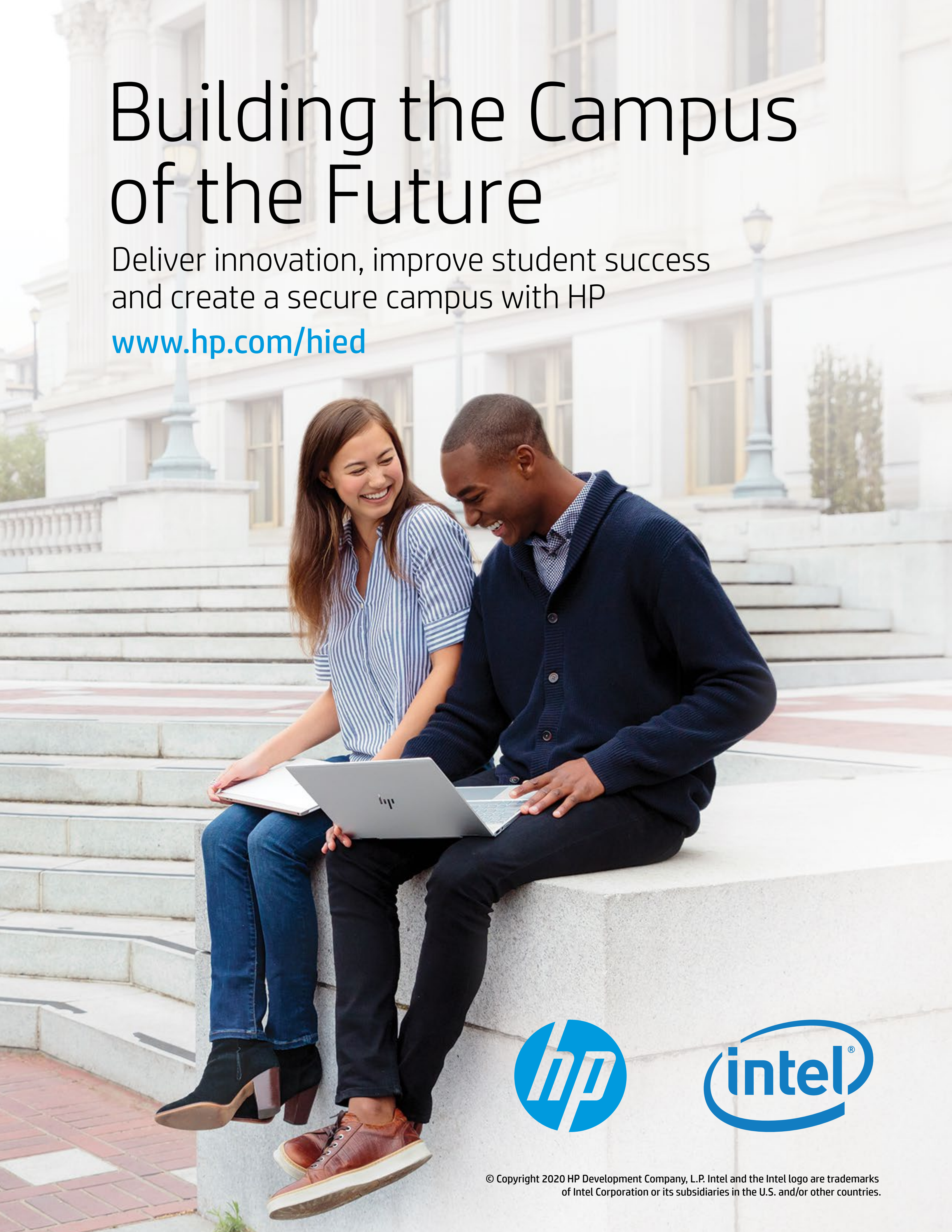
WITH SUPPORT FROM hp

THE CHRONICLE OF HIGHER EDUCATION®

Building the Campus of the Future

Deliver innovation, improve student success and create a secure campus with HP

www.hp.com/hied



PENNSYLVANIA STATE U.

Managing a Changing Threat

Colleges rethink the role of the information security officer amid online breaches

Five years ago, when Pennsylvania State was forced to shut down its network for three days after malware attacks from China and elsewhere were detected at the colleges of engineering and liberal arts, experts called the breaches “a wake-up call for higher education.”

In the years that followed, Penn State reshaped its management hierarchy specifically to strengthen its ability to withstand cyber threats. The university took the advice of an independent auditor and changed its line of reporting to reflect accountability practices in the private sector that have worked to limit the number of network intrusions.

In doing so, Penn State bucked a longstanding trend. At most other large institutions, a chief information security officer, or CISO, who monitors systems for signs of phishing, ransomware, viruses, and other breaches, reports to the chief information officer, or CIO. The CIO, who is responsible for purchasing and installing campus information systems, is in turn accountable to the president and the governing board. But too often, experts say, both IT-focused positions exist in their own organizational silo.

Penn State worked to change that. The university made the CISO position answerable to academic and financial officers and placed it on the same organizational rung as the CIO. And it expanded the information-security position to include other facets of university management, breaking it free from the IT silo.

"The CISO now participates in many aspects of university governance, not just IT governance," says Donald J. Welch, interim vice president for information technology and chief information officer at Penn State (and formerly chief information security officer). "Because the CISO does not report to the CIO, security is seen as a university problem and not just an IT problem."

Penn State's arrangement is different — and so far, rare. But it reflects an emerging reality for colleges awash in information and concerns about how to manage and protect it.

Penn State changed its administrative structure to prioritize cyber-security threats. Here, Donald J. Welch, its interim vice president for information technology and chief information officer, updates university staff about information technology.

BRIAN REED

A RISING NEED FOR CISOs

Institutions battle an ever-growing cyber menace. Countries not friendly with the United States regularly scan campus sites and databases for sensitive national-security information. Well-backed cybercriminal organizations search for sensitive and valuable personal and research data. Colleges and universities need management structures sturdy enough to meet and fend off dangerous, ever-changing, possibly costly attacks.

Around 40 percent of institutions have hired staff members solely responsible for anticipating and monitoring online security hazards, according to a 2019 study compiled by Educause, a nonprofit association that aims to help colleges find and put IT solutions into effect.

And that proportion may be on the rise. A survey conducted by the Leadership Board for CIOs in Higher Education found that nearly two in three institutions worldwide have hired CISOs, an increase of 10 percentage points from a decade ago.

Colleges that have created and staffed top information-security positions vary by type, the study found. Ninety-eight percent of research institutions have hired CISOs. Large universities and those with multiple schools are also likely to have a high-ranking administrator monitoring information security. But only about half of community colleges and small colleges have created those positions.

"Size makes a big difference, even at those levels," says Michael Zastrocky, executive director of the Leadership Board. "Large community colleges are more likely to hire CISOs than small ones. Generally, the more complex an institution is, the more likely it is that they'll have someone in that role."

Smaller colleges are less likely to have a management-level person who does a CISO's job. Often they task someone within the IT office to run security while attending to other duties as well. Others, such as Franklin & Marshall College and Susquehanna University, have begun to merge their cyber-security efforts. "They can't afford to hire a security expert from outside academia, or outsource that function, as larger schools have done," Zastrocky says.

By and large, he adds, information-security hierarchies at colleges and universities have remained roughly the same during the past decade. Nine in 10 higher-ed CISOs answer to the CIO, according to the Leadership Board's survey. Rarely are the two positions at the same level, as they are at Penn State.

AN EVOLVING ROLE

But two harbingers of change have emerged simultaneously: Institutions are creating some wrinkles in their management structures in response to the growing threats to privacy, and some have begun to break information-security officers and teams out of IT silos.

Though a typical college CISO has retained the same place within an organization, the position has risen in stature. More often these days, CISOs are entrusted to handle higher-level duties than before, including notifying board members of cyber-security concerns. And CISOs now are much more likely to move upward to the CIO spot.

"The CISO position isn't just about tech anymore," Zastrocky says. "A CISO needs to educate the entire campus community about cyber threats and how to deal with regulations. That includes the students — you need to constantly remind them that the device they hold needs to be used safely."

The CISO's job has morphed from one that focused on erecting firewalls and otherwise securing networks to one that assumes the role of a so-called cyber-security ambassador. Now many CISOs are expected to actively help key campus actors do their work.

At the University of Michigan, cyber-security officials aim to build relationships with faculty members to help them work more freely and efficiently. "Colleges, with their open and decentralized structure, are tremendously difficult institutions to secure," says Sol Bermann, CISO at

U. OF MICHIGAN

Sol Bermann (R), the chief information-security officer at the University of Michigan, and Florian Schaub, assistant professor of the university's School of Information, organized a daylong symposium on campus data privacy.

Michigan. “Yet we need to do more than provide that function. How, as a CISO, am I empowering researchers to reach any available database or website? How do I appropriately sell the idea of information security to tenured faculty? The goal is to make the flow of information both as free and secure as possible.”

Michael Corn, CISO at the University of California at San Diego, agrees: “If I can help a researcher do their work better while helping them protect their intellectual property, I’m helping the university achieve its mission.”

That melding of pedagogy, research, and security extends even further.

“Both CIOS and CISOs are moving toward becoming business assets,” says Brian Kelly, director of the cyber-security program at Educause. “They’re being asked to do more to help with student recruitment, retention, and how institutions are positioning themselves for the future. There’s a growing recognition that the CISO’s office isn’t the office of ‘no,’ as it has been seen in the past, but the office of ‘know.’”

Some institutions are now concerned about a related issue: privacy. In the past five years or so, many more colleges have hired chief privacy officers, or CPOs, to protect employee and student information, and to handle compliance with federal regulations — including the Family Educational Rights and Privacy Act (Ferpa), the Health Insurance Portability and Accountability Act (Hipaa), and the Sarbanes-Oxley Act, which applies to accounting and other business matters — along with emerging regulatory protocols, like the California Consumer Privacy Act.

Though there were only a handful of college privacy officers a decade ago, 41 of them now take part in an invitation-only email list run by Educause, Kelly says.

Institutional efforts to guarantee and secure privacy are evolving in a different direction from information management. CPOs often report to the chief legal counsel or compliance officer rather than to the CIO. “Privacy is becoming a separate issue,” Zastrocky says. “It’s not just about tech. It’s about protecting people’s information and their right to privacy, and being under compliance.”

Campus cyber-security programs may be becoming more specialized by institution type, observers say. Some research institutions that include campus hospitals or medical centers, like Johns Hopkins, are putting their CISOs under a risk-management superstructure. Such arrangements are becoming more common.

“If I can help a researcher do their work better while helping them protect their intellectual property, I’m helping the university achieve its mission.”

“For me, the elevation of risk-management people in the hierarchy is far and away the development I’ve noticed most,” says Darren Lacey, CISO at the Johns Hopkins University and Johns Hopkins Medicine. “They have influence with the top people that CISOs don’t. Enterprise risk-management programs have become a real thing at research universities.”

Some observers say that, despite the heightened emphasis on cyber security and the heightened role of CISOs, colleges may still be falling short on keeping their information safe. No matter what management system or structure they use, colleges face threats that advance at unprecedented rates.

“In all candor, higher ed isn’t moving at the pace it needs to in order to deal with this growing risk profile,” says Bradley Wheeler, vice president for IT and CIO at Indiana University. “State actors and criminal enterprises have all this connectivity. The bad guys are organized, industrialized, and automated. That’s just the world we live in.”

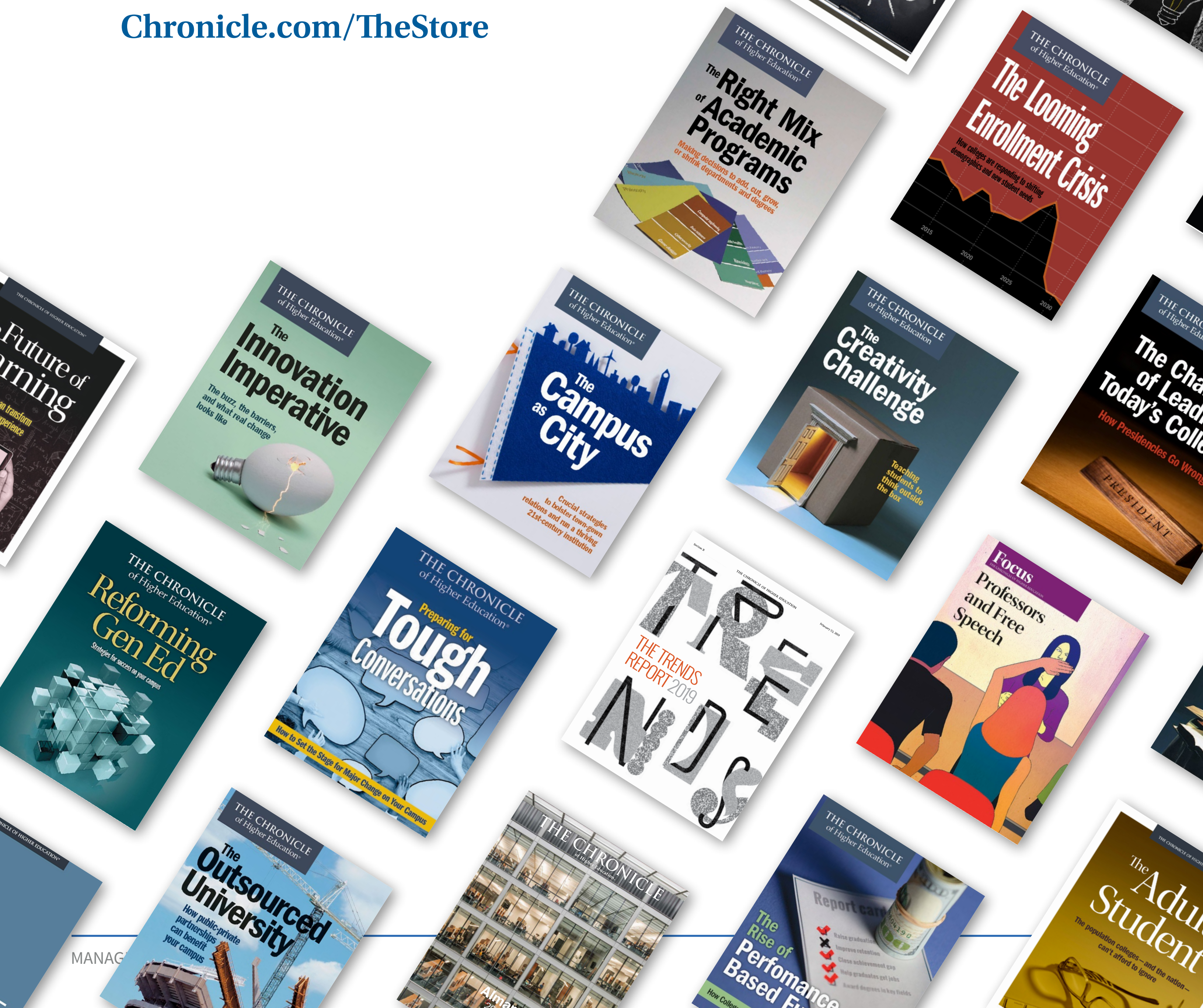
Questions or comments about this report? Email us at ci@chronicle.com.

THE CHRONICLE OF HIGHER EDUCATION

Explore the Store

No matter your area of expertise or where you are in your career, the right information is critical to succeeding in a rapidly changing world. Visit the Chronicle Store to get more of the essential tools, data, and insights you need to make the best decisions for your students, your institution, and your career.

Chronicle.com/TheStore



THE CHRONICLE
OF HIGHER EDUCATION®

1255 Twenty-Third Street, N.W.
Washington, D.C. 20037

(202) 466-1000 | Chronicle.com