Innovation in Higher Education

What is your campus security posture in the age of AI?

Colleges and universities must reevaluate their security postures as they arrive in the era of AI. Here's help for getting started.

AI is propelling rapid innovation and helping many campus teams deliver new insights and opportunities. Simultaneously, the risks posed by AI-driven cyberthreats, along with the emerging, unknown AI use cases that empower bad actors, are at an all-time high. As shadow AI proliferates on and off campuses, stretched-thin IT teams struggle to define or make sense of the actual scope and depth of the cybersecurity risks they face, and what new protections will be required. IT teams are now scrambling to take up the extensive AI cause.

PRESENTED BY: CAMPUS TECHNOLOGY

SPONSORED BY: Spectrum BUSINESS®

Breaking down those challenges into functional IT areas will help teams understand where immediate focus should be aimed, so that appropriate protections may be put in place while maintaining tolerable budgetary requests. Prioritizing and halting risks will help teams gain more solid footing as they evaluate where else AI might serve future campus needs. However, this must be accomplished without jeopardizing proper data governance, controls, and compliance policies as well as access, identity, and other cyber controls.

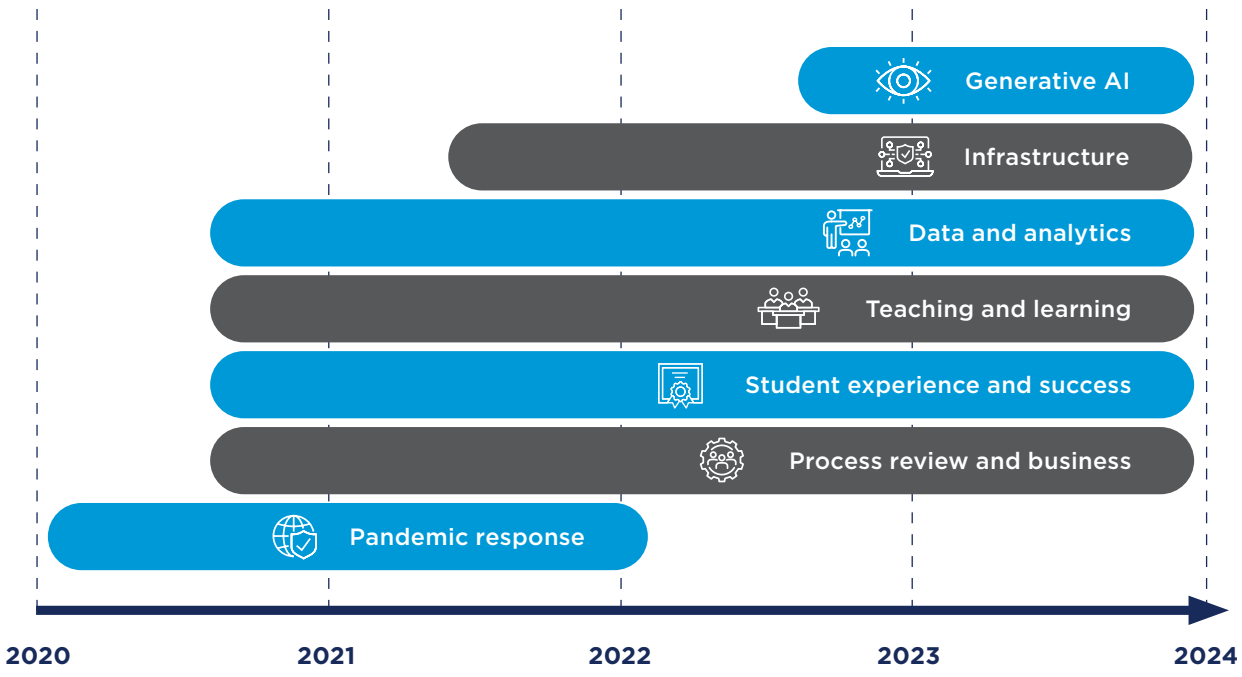
Up-to-date policies reign

A landmark study from EDUCAUSE, the "2024 EDUCAUSE AI Landscape Study," found that many institutions are now revising or creating new policies to address a wide variety of AI-related issues: Respondents (58%) said their institutions were either revising existing policies, creating new ones, or both; and 73% said that their AI-related policies are extremely permissive, somewhat permissive, or neutral, rather than restrictive. Colleges and universities have also begun the arduous work of strategic planning around AI, prompted primarily by student use of AI in their courses (73%), and by the risks of inappropriate uses of AI technologies (68%). Other respondents noted that their institutions are undertaking the work as preparation for students' workforce readiness. As one noted, "AI knowledge and use will be skills our students will need. We view this as an expansion of our digital literacy commitment to our students."[1]

As colleges and universities set their own policies and guidance about AI, governments and other oversight bodies continue to establish or revise their own. Keeping pace with shifting guidance and regulations while responding to questions around how to interpret new guidance will be required of risk management, IT, and cybersecurity teams.

Gartner advises preparation for three major types of risk: regulatory, reputational, and competencies.[2] While most colleges and

CATALYSTS OF INNOVATION IN HIGHER EDUCATION



SOURCE: GARTNER 798155_C

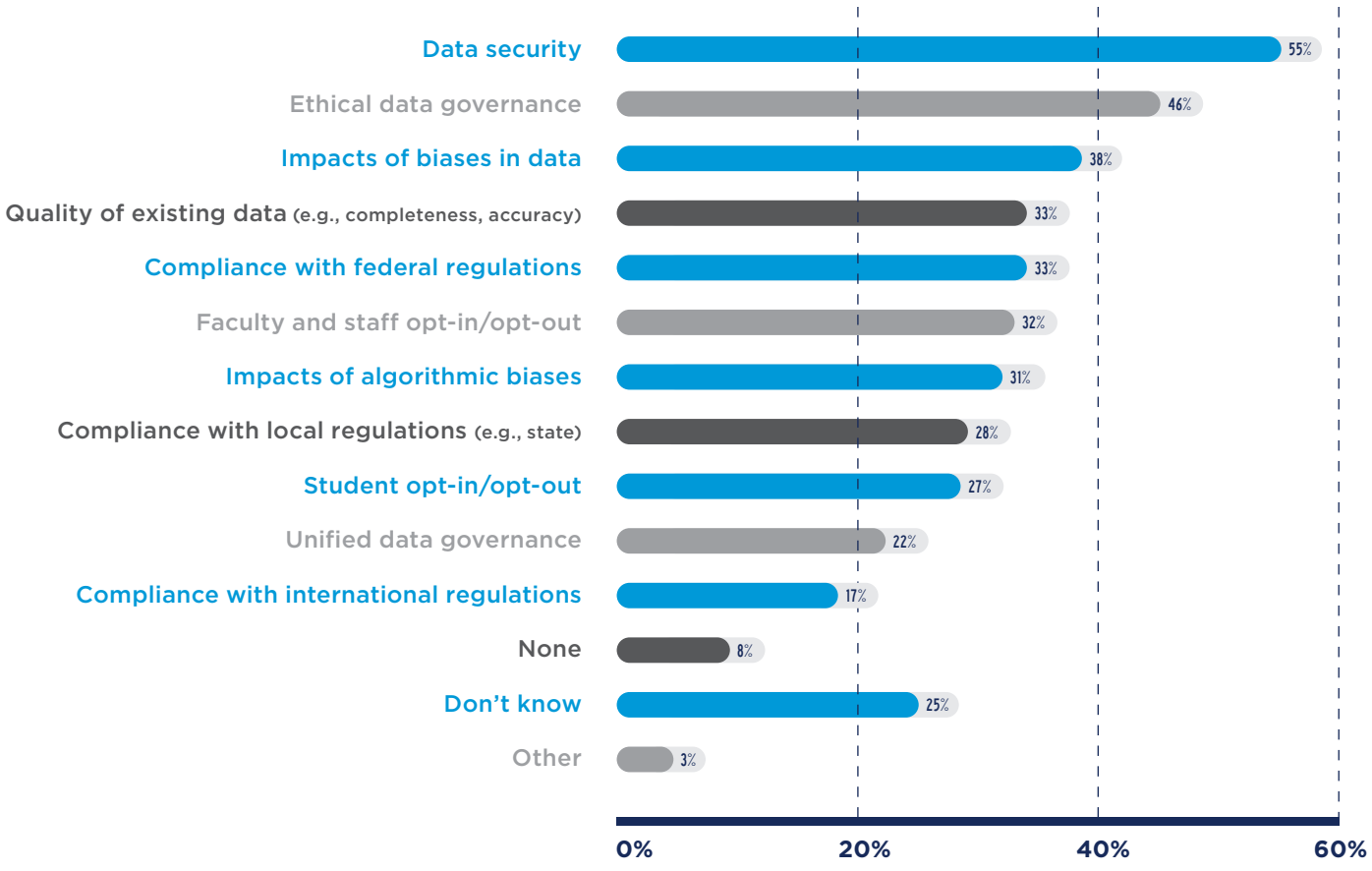
universities stand all too familiar with managing reputational risks in light of data breaches and other cyberattacks, competency-related risks may catch some institutions off guard.

Comprehensive policy and risk management evaluation will require diverse perspectives and input from every campus stakeholder group: legal, administration and executive leadership, faculty and students, IT, cybersecurity, facilities, and public safety — essentially any group that not only has the potential to use new AI tools but also stands as a target for breaches and other AI-driven risks. They must work together to define goals, identify and agree on acceptable or supported AI applications, and ensure everyone understands what will be required from a maintenance and infrastructure perspective.

All of this must be addressed even as institutional stakeholders remain skeptical that appropriate data privacy and protections are in place, as EDUCAUSE's study reveals. Only 18% of respondents felt that their institutions have the appropriate technology in place to properly ensure the privacy and security of data used for AI.[3]

"AI threats and compromises (malicious or benign) are continuous and constantly evolving, so set principles and policies for AI governance, trustworthiness, fairness, reliability, robustness, efficacy and privacy," Gartner's guidance states. "Organizations that don't are much more likely to experience negative AI outcomes and breaches. Models won't perform as intended, and there will be security and privacy failures, financial and reputational loss, and harm to individuals."[4]

AI-RELATED CYBERSECURITY AND PRIVACY CONCERNS



SOURCE: EDUCAUSE, "2024 EDUCAUSE AI Landscape Study," 2024

Managing it all

Where can institutions turn to make sense of all the new IT needs brought about by AI? Small, medium, and large-sized institutions all stand to gain from the experience and insight available through managed services.

Managed services play a valuable role in driving exceptional student and stakeholder experiences through:

- **Always-on support and troubleshooting**
- **Expected operational expenditures (OpEx) versus variable capital expenditures (CapEx) and outlays**
- **Up-to-the-minute insight into risks and global cyberthreats**

Managed services allow institutions to readily deliver seamless, productive, and effective campus experiences while helping teams maintain focus and efforts on driving new initiatives, like how to train for and deploy burgeoning AI tools and resources or training necessary skills, despite global IT staffing shortages and training gaps.

The ability to select specific support needs and choose from flexible service models helps two- and four-year institutions — from community colleges to the smallest private and largest state-funded R1 universities — customize solutions that will help them overcome ongoing digital transformation hurdles.

Powering and protecting it all

Teams will always need to consider AI's dual-sided nature promoting massive opportunities while also bringing new risks to light. Preparing campus infrastructure to deliver on AI's promise means taking a hard look at existing tools, bandwidth and throughput needs, storage and compute power, in addition to integrations, interoperability, and strategic edge resources.

When new AI solutions are brought online, networks suffer added strain and impacts to bandwidth, all of which impact user experience.

- Can the network handle greater amounts of data transmissions?
- Can campuses adequately scale data-intensive operations?
- How should access be handled?
- Will new tools fit or comply with a zero-trust framework?

Opportunities to harness AI

Leveraging new AI tools to manage risks and gain insights into network activities and risks presents opportunities for delivering greater value.

As campus teams struggle to manage the growing volume of new vulnerabilities making their way to networks and edge devices every day, turning to AI-powered solutions allows deeper analysis of device, server, and end user activities, helping to identify anomalous or unusual behaviors. AI holds great promise for protecting institutions against vulnerabilities they are unaware of even before they are officially reported and patched.

The benefits of automating AI in cybersecurity

Improve efficiency

Pairing cybersecurity with AI results in faster data collection. This makes incident management response more dynamic and efficient. It also empowers security professionals to focus on more strategic activities that add value to the organization.

Respond rapidly

AI can respond faster to risks than what's otherwise possible through manual analysis, mitigating and prioritizing threats based on pre-defined actions or anomalies, isolating and cordoning off systems, applying patches promptly, blocking traffic and more.

Formalize procedures

Automating cybersecurity helps organizations identify and correct potential deficiencies in their security strategy. In this way, they are able to implement formalized procedures that can result in more secure IT environments.

[1, 3] EDUCAUSE, 2024 "EDUCAUSE AI Landscape Study," 2024

[2] Gartner, "GenAI Planning Workbook," 2023

[4] Gartner, "Building a Value-Driving AI Strategy for your Business," 2025

Is your IT advancing in-demand campus initiatives?

From dorms to research and computing labs and everywhere else on and off campus, students, faculty, and staff demand always-on connectivity. To deliver exceptional experiences critical to recruiting and retention, and meet demands to deliver all the bandwidth required to power the latest AI/ML tools, flexible, scalable, and secure digitals will be required.

Spectrum Business® empowers colleges and universities to transform the student experience with networking, security, communications, collaboration and TV technology solutions. Our dedicated education IT experts serve hundreds of colleges and universities nationwide with a network engineered for exceptional performance, end-to-end accountability and 100% U.S.-based support, available 24/7/365.

Discover how Spectrum Business can help you modernize your IT infrastructure to support AI: enterprise.spectrum.com/highered