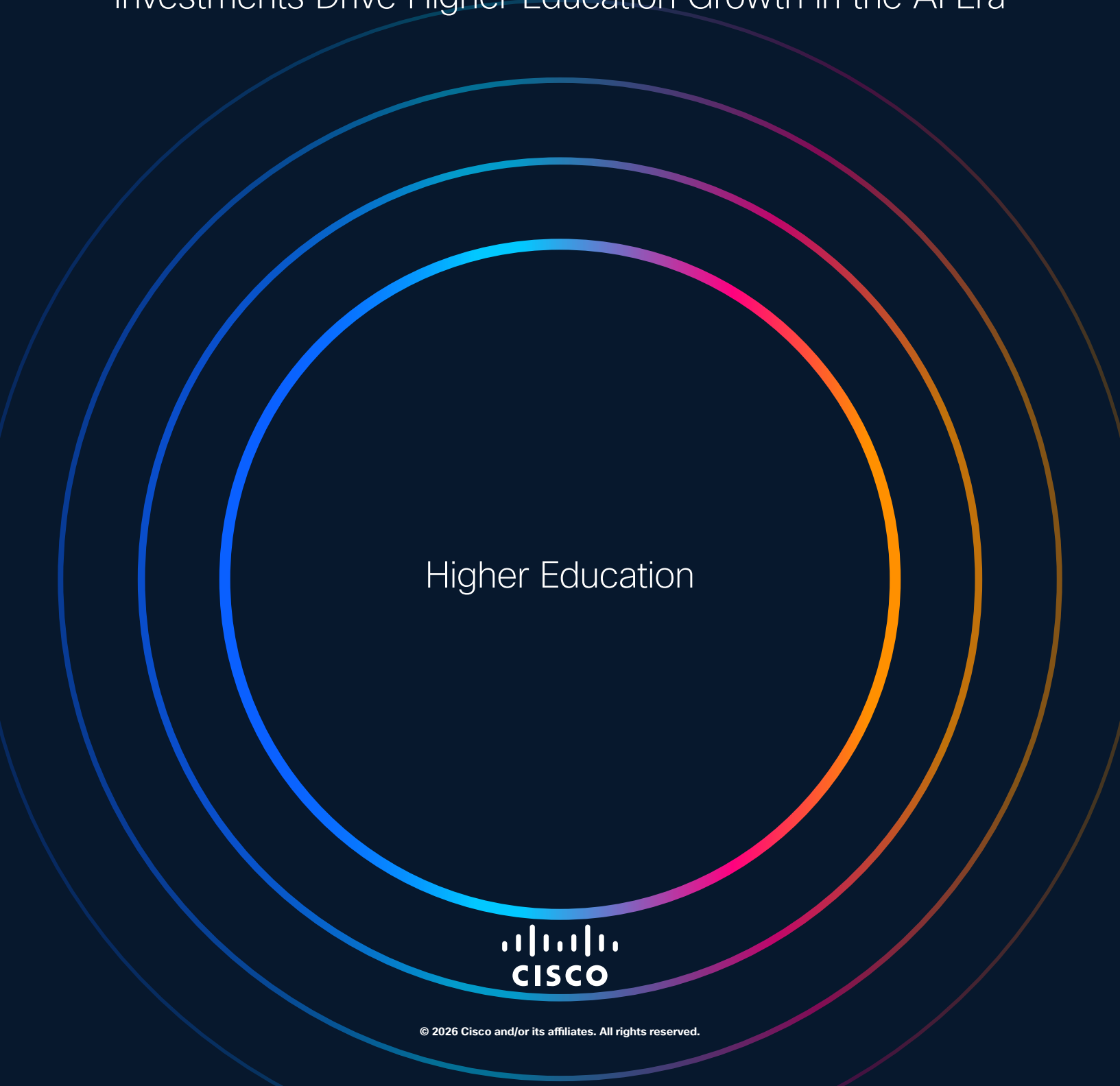
State of Wireless 2026

Unlocking the Multiplier Effect: How Strategic Wireless Investments Drive Higher Education Growth in the AI Era



Executive summary

University campuses have undergone a fundamental transformation in how they view wireless networks. What once served as a convenience for students between classes now represents a digital backbone that supports every aspect of academic life.

From streaming lectures to thousands of remote learners to sophisticated research instruments transmitting real-time experimental data, wireless infrastructure determines whether institutions can deliver on their educational mission. When networks fail during final examinations, the consequences ripple across the entire institution: assessments are delayed, student anxiety escalates, and administrative credibility erodes. When security incidents compromise student records, universities face not only regulatory penalties but lasting damage to the trust that defines their relationship with students and families.

The data confirms what university leaders already know. Nearly three quarters of institutions report that wireless investments have had a positive impact on operational efficiency, while 77% point to improvements in staff productivity and 73% describe stronger engagement with students and stakeholders. These results matter particularly in higher education, where institutions balance competing demands: excellence in teaching and research, fiscal responsibility in an era of constrained budgets, and accountability to diverse constituencies. Wireless infrastructure has become the connective tissue enabling universities to meet all these expectations simultaneously.

Yet the wireless opportunity arrives wrapped in a challenge that grows more pressing each year. Artificial intelligence promises to transform how universities operate: adaptive learning platforms that personalize instruction for each student, research tools that accelerate scientific discovery, operational systems that optimize everything from energy consumption to course scheduling. But deploying these AI applications demands wireless networks that perform at levels most campuses cannot currently support and simultaneously amplifies the very obstacles preventing universities from modernizing their infrastructure.

Our report examines this paradox in higher education institutions. It demonstrates how strategic investment in wireless infrastructure creates a multiplier effect, where a single network upgrade generates simultaneous improvements across multiple dimensions: student satisfaction, research output, faculty effectiveness, and financial performance. The report also reveals three interconnected barriers that stand between universities and unlocking the potential of wireless. Operational complexity forces IT teams into endless reactive firefighting. Security threats multiply faster than institutions can deploy countermeasures. Talent shortages leave universities competing for skilled professionals in a labor market where wireless expertise commands premium compensation. Universities that confront all three challenges together see dramatically higher returns. Those attempting to solve problems in isolation remain stuck in patterns that resist modernization and drain resources.

This report is grounded in Wi-Fi as the primary enterprise connectivity layer, while examining the broader wireless ecosystem it enables, including AI-driven applications, IoT and OT environments, and emerging enterprise use cases.

The opportunity:
Wi-Fi as a strategic growth engine for higher education

Wireless investment patterns in higher education tell a compelling story about institutional priorities. Over the past half decade, universities have channeled substantial resources into network infrastructure, recognizing the direct connection between connectivity performance and outcomes that matter: learning effectiveness and research breakthroughs, leading to stronger competitive positioning.

The investment trajectory shows no signs of slowing. A quarter of universities increased wireless budgets by more than half during the past four to five years. Looking forward, nearly one third (32%) anticipate budget growth exceeding 50% over the next four to five years. These figures reveal that universities are treating wireless not as overhead but as strategic infrastructure comparable to laboratories, libraries, and learning spaces.

The investment reflects recognition of what wireless infrastructure enables across campus. Students expect uninterrupted connectivity as they move between halls, libraries, and outdoor spaces, accessing materials, joining discussions, submitting assignments, and collaborating without thinking about the network behind it. Faculty lean on wireless to support hybrid classrooms, real-time polling, and cloud-based simulations once unimaginable. Researchers depend on wireless links to collect sensor data, monitor equipment, and share findings globally.

Beyond these established patterns, emerging applications show new possibilities: autonomous robots delivering materials, smart buildings optimizing energy and air quality,

and analytics platforms using wireless cameras to track movement, reduce bottlenecks, and guide facility design.

Universities are leveraging wireless across an array of use cases that span the entire institution.

The business case for wireless modernization emerges clearly from institutional experiences. Three quarters of universities report operational efficiency improvements, 77% describe gains in employee productivity, and 73% point to stronger engagement with students and other stakeholders. These improvements compound when universities align wireless investments with broader institutional strategy. A network upgrade intended to deliver increased computing power for research simultaneously enables richer learning experiences, more efficient administrative processes, and better facilities management. This multiplier effect distinguishes wireless infrastructure from investments delivering benefits in only one dimension. Modern wireless infrastructure generates simultaneous returns across student satisfaction, research productivity, faculty effectiveness, and financial performance.

Infrastructure decisions determine which possibilities universities can pursue. Aging wireless standards buckle under the combined weight of device density, bandwidth requirements, and latency sensitivity. Only 11% of universities have fully deployed Wi-Fi 6E or Wi-Fi 7 so far, though 66% plan implementation within the next year. This adoption trajectory reflects growing recognition that the 6 GHz spectrum provides the clean bandwidth required for emerging applications: virtual reality learning experiences, high-throughput research computing and distributed IoT sensor networks throughout campus facilities. Universities deploying 6 GHz spectrum demonstrate substantially higher rates of AI application adoption compared to institutions relying on older standards, suggesting that infrastructure modernization functions as a gating factor for innovation.

Higher education institutions are leveraging wireless across a variety of use cases

	Currently deployed (%)	Planning to deploy (%)
Real-time Asset and Equipment Tracking	43%	54%
AI Applications and Workloads	49%	50%
Internet of Things	50%	48%
Operational Visibility and Flow Analytics	50%	47%
Customer and User Experience Enhancement	54%	46%
Guest Wireless	53%	46%
Supply Chain and Inventory Intelligence	50%	46%
Physical Security (CCTV)	53%	45%
Remote Worker Connectivity	54%	43%

Current footprint = Deployed + Pilot stage
Future expansion = Planned next year + Planned in next 2–5 years

The wireless AI paradox in higher education

A striking tension shapes wireless strategy in universities today. Artificial intelligence is simultaneously the most compelling reason to invest in wireless infrastructure and the source of the most daunting obstacles preventing universities from capturing the value of that investment.

Consider first the opportunity side of this equation. Universities deploying AI applications view wireless infrastructure fundamentally differently than institutions where AI remains largely theoretical. Among organizations actively running AI workloads, 62% of leaders characterize wireless as strategically critical to their mission, compared to 46% among institutions not yet deploying AI. This perception gap reflects concrete experience of how AI applications stress networks. Adaptive learning platforms need real-time access to student data from LMSs, assignments, and interaction logs. AI-driven research relies on rapid retrieval of terabyte-scale datasets. Campus systems predicting at-risk students, optimizing schedules, or monitoring facilities all depend on networks with consistent, low-latency performance.

The same AI technologies enabling breakthroughs in personalized learning simultaneously drive operational complexity to overwhelming levels. Nearly every university (97%) reports escalating complexity in wireless operations, much of it stemming from AI workloads. AI also introduces sophisticated security threats that evolve faster than defenses can adapt. Meanwhile, AI intensifies competition for technical talent, drawing skilled professionals away from wireless roles into positions focused explicitly on artificial intelligence and cybersecurity.

The paradox poses acute challenges in higher education because failures reach far beyond disruption. Network lag can derail exams, delay data-intensive experiments, and block access to resources during assessment windows. Security breaches compromise student records, expose research data, disrupt exam administration, and trigger costly violations. The resulting threats to integrity, compliance, and institutional reputation make the wireless AI paradox one of the most consequential challenges facing university leaders.

Barrier 1: Operational complexity overwhelms current capabilities

Operational complexity in university wireless environments has reached levels that fundamentally alter how IT teams function. Nearly every wireless leader in higher education (97%) describes complexity as escalating, not merely as a temporary challenge but as a structural shift in the operational landscape.

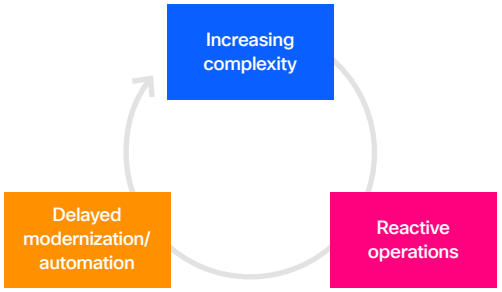
Three factors drive this complexity spiral. Mission-critical workloads, increasingly incorporating AI applications, rank as the leading contributor for nearly half (48%). Learning management systems supporting thousands of concurrent users cannot tolerate connectivity loss during high-stakes assessments. Research instruments collecting experimental data demand network excellence. AI applications require uninterrupted access to institutional databases.

At 42%, security is the second biggest contributor to complexity. This reflects the expansion of attack surfaces as thousands of personal devices connect daily, guest access accommodates visitors and prospective students, and IoT sensors proliferate throughout campus infrastructure. Client unpredictability contributes at 37%, driven by usage patterns unlike any other environment: students migrating constantly between lecture halls and study spaces, faculty accessing systems from home offices, researchers connecting from field sites often on different continents.

Operational strain manifests in metrics university IT leaders track constantly. Nearly half (48%) say their teams field at least 50 wireless support tickets weekly. This volume translates to hundreds of hours each month spent managing issues rather than advancing strategic initiatives. Time allocation patterns reveal an even more concerning reality: more than half of wireless teams (53%) spend the majority of their hours on reactive troubleshooting and incident management. They address problems as emergencies arise rather than preventing issues through systematic planning and proactive optimization.

A self-reinforcing pattern emerges from these dynamics. Complexity generates reactive work. Reactive work consumes all available capacity. Strategic initiatives get postponed: infrastructure modernization, staff training, certification programs, automation implementation.

Deferred modernization allows complexity to persist and intensify. The cycle repeats, trapping teams in reactive patterns precisely during periods when network performance matters most: examination windows, research grant deadlines, enrollment cycles.



Visibility gaps compound every other challenge universities face. Nine in 10 institutions report blind spots that impede effective troubleshooting. Client visibility ranks as the most common gap (48%), followed by application and cloud visibility (44%) and packet-level visibility (40%). Without comprehensive insight spanning every network layer from access points through applications, IT teams struggle to isolate problems rapidly across environments encompassing residence halls, lecture facilities, research laboratories, libraries, and administrative buildings.

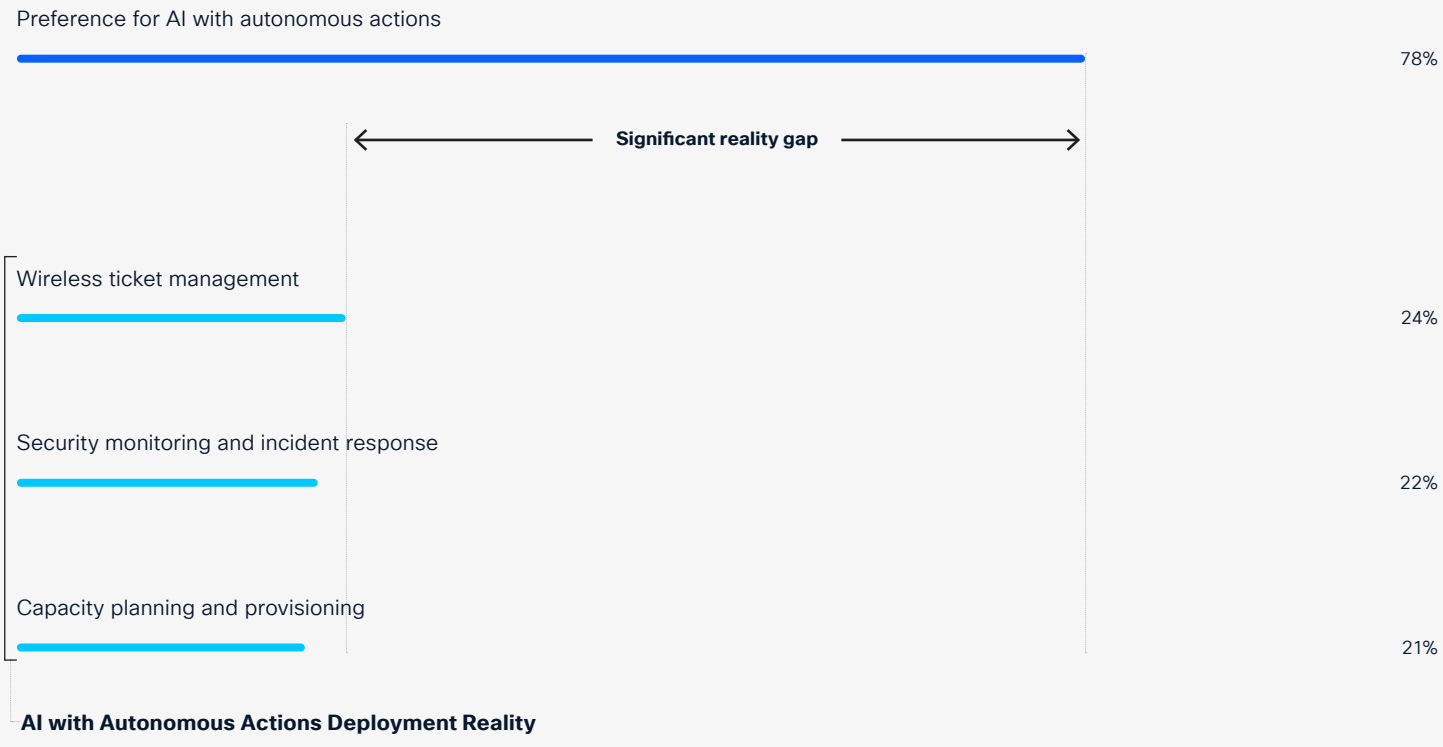
Visibility limitations create a pattern familiar to every university IT professional: wireless networks take the blame for problems originating elsewhere in the technology stack. More than half of university respondents (57%) report that at least 10% of incidents blamed on wireless actually originate elsewhere. Each misdiagnosis consumes an average of 18 hours across teams. These wasted hours delay attention to actual problems while service degradation persists during examination periods and research deadlines.

Faced with escalating complexity, university wireless leaders see AI automation as the most viable solution. More than three quarters (78%) would prefer AI systems to handle routine wireless operational tasks fully or mostly. The value proposition is straightforward: automation liberates IT professionals from repetitive ticket management, enabling focus on strategic work directly supporting academic missions. AI systems can detect and resolve many incidents before they impact users, maintaining service continuity during high-stakes academic periods when degradation carries the greatest impact.

A substantial gap separates aspiration from implementation. Wireless ticket management automation exists in only 22% of universities. Security monitoring and incident response automation stands at 24% while just a fifth (21%) of universities have automated capacity planning and provisioning. University leaders recognize AI automation as the solution to complexity while simultaneously lacking resources, expertise, or organizational capacity for scaled deployment. The implementation gap is wider in higher education than in many other sectors, reflecting the fiscal constraints and competing priorities that define university environments.

Performance data from universities implementing AI automation reveals substantial benefits, though. Organizations deploying autonomous AI actions save an average of three hours and 20 minutes per person every day. These institutions are four times more likely to characterize network operations as very simple and their ticket resolution times are 12% faster than manually operated counterparts. Extending these results across all universities would free thousands of hours monthly for work advancing academic priorities. Yet scaling is constrained by the very problems automation would solve: overwhelming complexity and talent shortages. Early adopters of AI automation gain competitive advantage, particularly in attracting students and faculty whose expectations for seamless digital experiences reflect their experiences with consumer technology platforms.

The AI gap in higher education: Desire versus reality



Barrier 2: Wireless security under siege

Security threats targeting university wireless networks have intensified along every dimension: frequency, sophistication, and consequences. More than four in five universities (84%) experienced at least one wireless security incident over the past year. More than four in 10 (41%) report that wireless threats have escalated over the past two years, and the outlook is even more troubling: 71% expect security incidents to rise further in the next two years.

University security threat environment

The threat landscape confronting higher education differs from other industries in significant ways. Five factors stand out as primary vulnerability drivers:

1. AI-generated or automated cyberattacks lead the list at 32%. These attacks identify network vulnerabilities across distributed campus infrastructure, adapt strategies in real time based on defensive responses, and operate at scales and speeds impossible for human attackers to match.
2. Budget and resource constraints rank second at 31%. Universities recognize security risks but often cannot deploy modern countermeasures due to competing demands on limited budgets.
3. Personnel shortages and limited bandwidth for security monitoring is a factor for 30% of respondents. Understaffed teams cannot maintain continuous surveillance across sprawling campus networks, amplifying every other vulnerability.
4. IoT and connected device proliferation stands at 28%. Sensors, research instruments, and smart building systems multiply across campus, each representing a potential entry point. Individual device vulnerabilities compound into aggregate network exposure.
5. Poor user practices, human error, and insider risks round out the top five at 25%. Universities face unique challenges securing networks when thousands of users connect personal devices daily, many with minimal security awareness or training.

Compromised IoT and operational technology devices create consequences beyond typical IT incidents. Over one third of universities (36%) report disruption from compromised devices, leading to corrupted research data, unsafe building conditions, or failed security cameras. These scenarios transcend IT operations, directly affecting academic integrity and campus safety.

Financial consequences reach levels that command attention from university leadership. More than half of institutions (53%) have absorbed financial losses from wireless security incidents. Among those experiencing losses, nearly half (49%) report costs exceeding one million dollars in the past year alone. These figures capture only direct costs: breach remediation, forensic investigation, incident response. Indirect costs compound the damage with loss of stakeholder trust affecting 42% of universities, the highest rate across all industries surveyed. Regulatory penalties and compliance consequences impact 34%. Reputational damage influences student recruitment and donor relationships in ways that persist long after incidents are resolved. In university contexts, stakeholder trust spans students, parents, faculty, alumni, donors, and community partners. Once compromised, trust rebuilds slowly if at all.

Financial losses from wireless security incidents in universities

Less than US$1 million	45%
US$1–10 million	22%
US$10–50 million	22%
Over US$50 million	5%

A troubling disconnect emerges in how universities assess their security posture. Four in five institutions (80%) report confidence that current measures adequately protect wireless networks. Yet simultaneously, 71% predict security failures will increase over the next two years. This contradiction likely reflects divergent perspectives between executive leadership and frontline technical staff. Executives tend to perceive organizations as adequately defended based on policies and investments approved. Technical staff managing networks daily understand threat evolution and defensive limitations more viscerally.

Three obstacles consistently impede security modernization in universities: implementation complexity, legacy infrastructure constraints, and performance concerns and interconnect with the broader challenges. Operational complexity makes security deployment difficult across distributed campus environments serving diverse user populations. Talent shortages leave institutions without the specialized expertise required for modern protocol implementation. Visibility gaps prevent security teams from fully understanding threat environments encompassing thousands of devices and connections.

These dynamics create a vulnerability gap that widens over time. Threats evolve and intensify while universities remain constrained by legacy systems, overwhelming complexity, and insufficient expertise. Security modernization proceeds slowly. Resilience erodes. Competitive pressure intensifies, particularly in higher education markets where security incidents immediately damage institutional reputation and influence prospective student enrollment decisions.

Barrier 3: Wireless competition for AI skills

Talent scarcity represents the third critical barrier universities confront. More than four in five institutions (83%) report difficulty hiring wireless professionals with skills matching modern network operation requirements. This extends beyond cyclical hiring challenges to structural problems affecting institutional capacity to maintain and modernize infrastructure supporting academic and research functions.

Competition for technical talent operates asymmetrically against wireless specialization. AI and machine learning rank as the top domain drawing talent away from wireless roles, identified by 48% of universities as a primary competitor for staff. Cybersecurity ranks second at 46%, offering high visibility and accelerated career progression. Data science and analytics attract 39% of potential wireless talent. Universities watch their most skilled wireless professionals migrate to positions perceived as more innovative, better compensated, and more closely aligned with institutional research and academic priorities.

University talent competition and hiring challenges

Domains attracting talent away from wireless

AI / Machine learning	48%
Cybersecurity	46%
Data science and analytics	39%

Primary reasons for difficulty in hiring wireless talent

Shortage of candidates with advanced wireless or AI-integrated skills	45%
Internal budget constraints or hiring freezes	38%
Geographic limitations or remote work challenges	37%

The underlying problem is straightforward but intractable. A shortage of candidates possessing advanced wireless or AI-integrated skills represents the primary hiring barrier for 45% of respondents. Labor markets simply lack sufficient professionals with deep wireless knowledge, particularly expertise combined with understanding of higher education requirements: diverse user populations, distributed campus architectures, stringent privacy regulations. Budget constraints and hiring freezes compound the problem at 38% of institutions. The resulting skills gap manifests in higher operating costs (42%), diminished morale among wireless staff (34%), and constrained innovation capacity (30%).

Talent shortages correlate unmistakably with poor outcomes. Universities struggling to hire wireless specialists anticipate security failures increasing at substantially higher rates than institutions facing no recruitment difficulty. They already absorb significantly higher annual costs from security incidents compared to universities with adequate wireless staffing.

Wireless operational resilience begins with certified expertise. Teams with deeper credentials deploy modern security protocols faster and more comprehensively. Universities where at least half the wireless staff hold technology certifications are 17% more likely to implement full WPA3 security, reducing exposure to attacks exploiting legacy protocols. They are also 17% more likely to deploy certificate-based or profile-based authentication, minimizing access conflicts and reducing troubleshooting volume during peak demand periods when students access resources for examinations and assignment submissions.

The strategic imperative is unambiguous. Universities investing early in talent development and certification accumulate competitive advantage as complexity escalates and specialized skills grow scarce. Institutions delaying investment until shortages become acute face substantially higher hiring costs, extended project timelines, and diminished modernization capacity. In higher education contexts where delayed modernization costs include both quantifiable financial losses from security incidents and immeasurable damage to academic experiences, talent investment becomes mission-critical.

Universities face a compounding talent challenge: they compete for professionals inherently attracted to academic and research environments. Many skilled wireless practitioners prefer university settings over corporate alternatives. Yet these same professionals increasingly gravitate toward roles in AI, cybersecurity, or data science offering more direct engagement with cutting-edge academic work. Universities positioning wireless roles as integral to research infrastructure and academic innovation improve their competitive standing for attracting and retaining specialized talent.

Conclusion

Universities confront a paradox ranking among the most consequential strategic challenges in higher education. Wireless infrastructure has become essential to excellence in teaching, learning, and research. AI applications promise to transform personalized learning, accelerate scientific discovery, and optimize campus operations. Yet capturing this potential demands that university leaders address three interconnected barriers simultaneously rather than sequentially.

Operational complexity traps IT teams in reactive patterns, consuming capacity needed for modernization precisely when academic demands peak. Security threats evolve faster than institutions can deploy countermeasures, jeopardizing institutional reputation and stakeholder trust. Talent shortages amplify both challenges while constraining resources available for solutions. Addressing barriers in isolation leaves the fundamental paradox unresolved. Universities modernizing infrastructure without implementing automation drown in reactive work during examination periods and research deadlines. Universities implementing automation without deploying modern security manage vulnerable networks efficiently while exposing sensitive student and research data. Institutions modernizing security without developing certified expertise deploy protective measures that staff cannot properly implement or maintain across distributed campus environments.

Conversely, universities addressing all three barriers together achieve substantially higher returns on wireless investment. They realize stronger operational efficiency improvements, enhanced student satisfaction, accelerated research output, reduced security incident costs, and improved faculty and staff satisfaction. The multiplier effect amplifies when all dimensions align: modern infrastructure enables academic innovation, automation liberates teams to support teaching and research priorities, robust security protects institutional data and stakeholder trust, and certified talent ensures sustainable operations adapting to evolving academic requirements.

The financial argument is compelling. Universities deploying modern wireless infrastructure, automation capabilities, security protocols, and certified talent demonstrate substantially higher likelihood of achieving strong wireless ROI. They absorb lower security incident costs, resolve operational problems faster, and achieve superior student outcomes translating directly into enhanced institutional reputation and competitive positioning.

The opportunity window for competitive advantage opens now. Institutions acting decisively and holistically in 2026 will establish wireless as the strategic foundation for academic excellence throughout the next decade. Universities that defer action will remain trapped in reactive cycles, absorbing escalating security incident costs, unable to capitalize on AI-driven transformation while peer institutions advance. In higher education where institutional reputation accumulates over decades but can suffer damage in moments, organizations moving first to resolve the wireless AI paradox will attract the most promising students, accomplished faculty, and competitive research funding in years ahead.

Methodology

This research comprised interviews with 6,098 organizations, including 292 in university education, across 30 markets. It was conducted in November 2025 by Sandpiper Research and Insights.

Research Scope

Respondent Profile: Interviews were conducted with 6,098 wireless decision makers and technical specialists in organizations with at least 250 employees. Six in 10 (61%) respondents work in organizations with annual turnover of at least US$100 million.

Americas — 22%

Europe, Middle East, and Africa — 28%

Asia Pacific — 50%

Geographic Coverage: Research covered 30 markets including Australia, Brazil, Canada, Chinese Mainland, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, United Arab Emirates, United Kingdom, United States, and Vietnam.

Industry Representation: Respondents worked across a range of industries including Business Services, Construction, Education, Engineering, Design and Architecture, Financial Services, Government and Public Services, Healthcare, Manufacturing, Media and Communications, Natural Resources, Real Estate, Restaurant Services, Retail, Technology Services, Transportation, Travel Services, and Wholesaling.

Timing: Research was conducted in November 2025.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**