Higher Ed Risk©

The magazine for news, trends, and insights supporting higher education leaders nationwide.

NAVIGATING UNPREDICTABLE CHANGE

READ MORE ON PAGE 13

SUMMER 2025

IN THIS ISSUE:

- Managing Mental Health
- Property Insurance Coverage
- AI Innovation & Governance
- Payment Card Industry Compliance
- Enterprise Risk Management
- Cybersecurity & Privacy
- Antitrust Suits

Don’t miss a risk!

Subscribe to our newsletter and magazine:

SCAN ME

HigherEdRisk.com

WELCOME TO

HigherEdRisk©

HigherEdRisk aims to bring greater visibility to the news, trends, and insights shaping the threats to higher education. Contributions are invited, but copies of work should be kept, as the magazine can accept no responsibility for loss. Contact editor@higheredrisk.com to seek permission or contribute to future editions.

Publisher: John Fees, Next Generation Insurance Group

Creative Directors: Jayme Wong and Rob Kubasko

Copy Editor: Brian Roper

Editorial Inquiries: tswift@higheredrisk.com

Subscriptions: subscriptions@higheredrisk.com

Advertising: advertising@higheredrisk.com

Letter from the Editor

To say that higher education is experiencing significant disruption is an understatement, but with disruption comes opportunities and risks. More than ever, higher education boards, fiduciaries, risk managers, and executive leaders will be called upon to make critical decisions with incomplete information to lead their institutions forward.

Similar to COVID, we are in another period of uncertainty; and the downstream risks hinge upon potential legislative changes that cannot only impact institutional finances but also student experience, research, and academic programming. It's time to view risk with a new lens and adjust risk management frameworks to the swings of the pendulum. This is not an easy task; but in doing so, there are opportunities to enhance institutional resilience.

One of the core principles of enterprise risk management is maintaining a broader perspective to identify risk. Only seeing one siloed view can create blind spots. Incorporating a risk management mindset at the executive and board levels will help connect the dots between risk exposures to facilitate more agile decision-making.

On another risk front, the constant flux of news headlines can generate a lot of angst. Mental health, particularly concerning students, has been frequently named a top risk by industry experts. The current macro-environment may heighten this risk, but the good news is there are tools to help. We must also recognize that mental health is not only a student risk but also a leadership risk. As we all navigate yet another "new normal," we must check in on ourselves as leaders. In fact, we have an article on this very topic.

Highlights of this issue include:

- In the article titled Breaking the Isolation, learn how executives can leverage tools to promote and foster sound decision-making amid great pressure and demand.
- Are you familiar with The Jed Foundation? Dr. Nance Roy's article helps university decision-makers to understand JED's important work and share its successful framework that nearly 500 schools have used to mitigate student mental health risks.
- Antitrust lawsuits are expensive, so it would be prudent to reduce your institution's risk by taking proactive measures.

As with our previous editions, I curate articles with interconnected themes. The key takeaways from this issue are:

- AI governance remains a top concern. How institutions manage this risk is key to combating bias and mitigating other ethical dilemmas.
- The complexity of risk management has reached a fever pitch, and enterprise risk management is essential to pave the path forward. Melissa Diaz from the University of San Francisco will share some insights if you would like to know where to begin.
- The contributing experts in this magazine prove that we can all be risk managers. Whether you are a board member, professor, lawyer, mental health professional, or Chief Information Security Officer (CISO), the value of risk management unites us all.

I cannot believe it has been eight months since our inaugural edition was released. This edition makes it our third issue! Thank you for joining us. I wish your institution much success and hope the articles in this issue provide you with risk intelligence to help your institution thrive.

As always, I welcome feedback and suggestions!

In service,

Tracey M Swift

Tracey M. Swift
Editor-in-Chief, ***HigherEdRisk***
tswift@higheredrisk.com

Contents

Citations below are for the article on page 4

1. https://www.law.cornell.edu/wex/sherman_antitrust_act#:~:text=Sherman%20Antitrust%20Act%20of%201890,of%20foreign%20or%20interstate%20trade
2. https://www.law.cornell.edu/wex/clayton_antitrust_act
3. https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act
4. https://www.justice.gov/atr/case/us-v-national-association-college-admission-counseling
5. https://www.justice.gov/atr/case/us-v-national-association-college-admission-counseling
6. https://www.reuters.com/legal/government/us-judge-approves-284-mln-settlements-financial-aid-litigation-2024-07-19/
7. https://www.forbes.com/sites/michaeltnietzel/2025/01/20/caltech-johns-hopkins-university-settle-in-financial-aid-lawsuit/
8. https://www.justice.gov/atr/media/1384596/dl?inline
9. https://www.justice.gov/atr/case/us-v-national-association-college-admission-counseling
10. https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/enforcers#:~:text=The%20injunction%20preserves%20the%20market's,banks%2C%20railroads%2C%20and%20airlines
11. https://policies.duke.edu/policy/duke-university-antitrust-policy/
12. https://ogc.stanford.edu/sites/g/files/sbiybj22406/files/media/file/stanford-antitrust-guidelines-memo_accessible.pdf
13. https://www.smu.edu/ola/briefingpapers/antitrust-compliance-guidelines

LEGAL RISK

Hillary Pettegrew, Esq. is a Senior Risk Management Counsel for United Educators (UE). Her areas of expertise include employment law, Title IX, and study-abroad issues. Before joining the Risk Research team, she practiced employment law and handled UE education liability claims.

Spotlight on the Risks of Antitrust Suits

Several well-publicized antitrust actions targeting education over the last five years have resulted in multimillion-dollar settlements. These cases highlight the importance of understanding the legal and financial risks that higher educational institutions face and how higher education leaders can mitigate them.

Educational Antitrust Issues

Higher ed institutions are subject to federal antitrust laws including the Sherman Antitrust Act[1], the Clayton Antitrust Act[2], and the Federal Trade Commission Act[3].

These laws seek to promote marketplace competition and prevent unfair business practices.

In 2020, the National Association for College Admission Counseling (NACAC)[4] settled a Department of Justice (DOJ) case over rules that allegedly violated the Sherman Act by restricting NACAC members' ability to recruit applicants and transfer students.

Private lawsuits filed in 2022 and in 2024 accused "elite" private institutions of colluding to limit financial aid awards to students[5]. Ten schools sued in the first lawsuit and settled in 2024 for $284 million[6], while two more reached settlement agreements in January 2025 worth over $35 million[7].

Other practices[8] may violate antitrust laws, including "anti-poaching" agreements (agreeing not to recruit faculty, other employees, or students from each other) and agreements to limit employee compensation or benefits. These agreements do not have to be formal, explicit, or written to violate the law. Sharing certain sensitive data, such as wage information, with other institutions also can violate antitrust laws.

Reduce Your Risk With Proactive Steps

Antitrust litigation is complex and costly. Increasing public anger over rising costs of education and a perceived absence of transparency from institutions may fuel future lawsuits.

To avoid anti-competitive practices and reduce your institution's chances of being sued for alleged antitrust violations:

Understand the Legal Landscape

Ensure your officials have a general understanding of antitrust law and how it may apply to your institution. This can help you spot potential problems and recognize when your institution needs legal advice.

The DOJ[9] and the Federal Trade Commission[10] enforce antitrust laws. They usually coordinate their investigations and focus on different areas. Both can impose significant fines for civil violations, and people impacted by antitrust violations can sue. The DOJ also can bring criminal prosecutions. This is rare; but in egregious cases, people involved in violations can face up to 10 years in prison.

Check Your Policy

Consider working with legal counsel to create a written policy[11] and/or guidelines[12] mandating employee compliance with antitrust laws and prohibiting certain conduct[13]. Your rules might, for example, require officials to make decisions about tuition and financial aid independently and without consulting or working with other institutions.

Consider State Laws

Most states have antitrust laws (modeled on but not necessarily identical to federal laws) applicable to commerce within their borders, and states often work cooperatively with federal agencies to pursue antitrust violations. State laws typically allow lawsuits by private individuals. In addition, state attorneys general can sue to enforce their own laws, or they might sue on behalf of the state's citizens to enforce federal antitrust laws.

While federal law generally preempts conflicting state law, most state antitrust laws were designed to complement rather than conflict with federal laws. As a result, an institution could potentially find itself facing separate lawsuits in federal and state courts over the same alleged anti-competitive conduct.

Train Personnel

Regularly train employees, especially those in admissions, financial aid, and human resources, to recognize and avoid risky conduct. What some might consider "cooperation" or "collaboration" between peer institutions could amount to unlawful collusion under antitrust laws.

During training:

- Review your relevant written policies or guidelines.
- Advise employees to avoid formal or informal agreements with other institutions regarding admissions practices (such as an explicit promise or implied understanding not to recruit students who commit to attending other institutions), tuition/financial aid packages, employee compensation packages, or sharing sensitive data.
- Explain how employees can report concerns related to antitrust issues.
- Emphasize the possible penalties for antitrust violations, including significant fines and the risk of serious, long-term damage to your institution's reputation.

BOTTOM LINE

Effective risk mitigation requires leadership commitments to understand the legal landscape, review policies, and train personnel. By prioritizing these strategic initiatives, institutions can help protect their financial health, avoid lawsuits, and mitigate reputational risk while aligning with evolving regulatory expectations. ◆

Citations on page three.

STUDENT MENTAL HEALTH

Dr. Nance Roy is a psychologist with over 30 years of experience who has dedicated her career to protecting the mental health of teens and young adults and reducing suicide. As the Chief Clinical Officer of the Jed Foundation and Assistant Clinical Professor at the Yale School of Medicine, Dept. of Psychiatry, she consults with high schools, colleges, and workplace/professional organizations across the country on effecting systems change, strategic planning, and implementing recommended practices that promote positive mental health.

Prior to her current role, she held leadership positions at several colleges to support student well-being. Dr. Roy is a recognized speaker and has been featured in major media outlets and publications, and has collaborated with national organizations devoted to promoting mental health. Dr. Roy holds a doctorate from Harvard University, master's degrees from the University of North Carolina and Harvard University, and a bachelor's degree from the University of Rhode Island.

Navigating the Risks of College Student Mental Health: Strategies for Risk Managers

Over the past decade, mental health challenges among college students have been well documented and continue to be a growing concern. Data from the 2023-2024 Healthy Minds Study revealed that 38% of undergraduates experienced moderate to severe depression, 34% reported mild to severe anxiety, 25% screened positive for suicidal ideation, 6% made a suicide plan, and 2.2% made a suicide attempt, with suicide being the second leading cause of death.

For students, their school community is a critical part of their support network and emotional safety net. When considering how best to protect the mental health of college students, it is important to remember that while college life can be exciting, it is not without stressors. Increased academic pressures, social adjustments, financial stress, and navigating the challenges that accompany increased independence can contribute to feelings of isolation, loneliness, anxiety, and depression. In severe cases, this can lead to self-destructive behaviors or suicide.

These risks not only impact students, but they also can pose significant risk to the academic institution. Institutional risk may take the form of decreased retention rates, possible liability if a student's mental health leads to self-injury, suicide, or a threat to the campus community. An institution's reputation may also be damaged if it failed to provide adequate support for students' mental health or failed to intervene appropriately when a student is in crisis.

The Jed Foundation's Comprehensive Approach

The Jed Foundation (JED), the nation's leading non-profit organization that protects emotional health and prevents suicide for teens and young adults, works directly with colleges, school districts, and high schools to put systems, programs, and policies in place to create a culture of caring that promotes student mental health and reduces risks for suicide.

In addition to working directly with schools, The Jed Foundation has partnered with United Educators, which offers liability insurance to colleges and universities to provide resources that promote mental health awareness and prevention. As part of that partnership, United Educators offers schools that work with JED a discount on their insurance premiums, reinforcing the message that protecting college students' mental health is an important step in mitigating risk on campus.

JED's Comprehensive Approach is grounded in the belief that promoting student mental health is a campus-wide responsibility and includes strategic domains that should be addressed in any community-wide effort to support mental health and reduce suicide. There are tactical activities within each strategic area (outlined below) that risk managers can promote to assist schools in supporting student well-being.

Risk Managers as Partners

As risk management becomes more of an enterprise discipline, risk managers can play an important role in mitigating the risk of student mental health challenges. Risk managers, as strategic partners, can help drive a comprehensive, cross-functional approach while positioning themselves as champions for student mental health initiatives across the institution.

Develop a Strategic Plan

Risk managers can be integral in promoting and developing a plan that addresses all aspects of student mental health, including prevention, early intervention, and crisis response. Such a plan makes clear that supporting student mental health is a campus-wide responsibility.

Identifying Students at Risk

Risk managers can help identify and implement targeted training programs for faculty, staff, and students on how to recognize when a student may be struggling, how to reach out and offer support, and how to know when and where to refer to professional help. Identifying early signs of struggle and offering early support can often avert a mental health struggle from becoming a crisis. Establishing centralized systems for faculty, staff, and students to report students of concern also allows the institution to effectively reach out to support students who may be struggling.

Risk managers can also help establish a care team that includes appropriate staff to review reports of students of concern, evaluate risk, and create an appropriate plan for outreach. This cross-functional approach enhances institutional responsiveness and mitigates risk through early identification and coordinated action.

Develop Crisis Response Procedures

Risk managers can partner with appropriate professionals on campus to develop clear protocols for responding to mental health crises, including training staff on how to de-escalate situations, responding to a death on campus, ensuring access to emergency services, and ensuring that medical leave and return-from-leave policies best support students when they need time away from campus to attend to their well-being.

Promote Means Safety

Risk managers can conduct annual environmental scans to identify potentially dangerous areas on campus where students could bring harm to themselves and implement strategies to reduce access. In addition, implementing measures to restrict access to potentially lethal means such as securing potentially dangerous chemicals or medications, as well as securing firearms if allowed on campus, is essential.

Be an Advocate for Providing Mental Health and Substance Abuse Services

Risk managers can advocate for readily available and accessible counseling services on and/or off campus that include triage systems, after-hours support, and access to teletherapy options if available.

Increase Help-Seeking

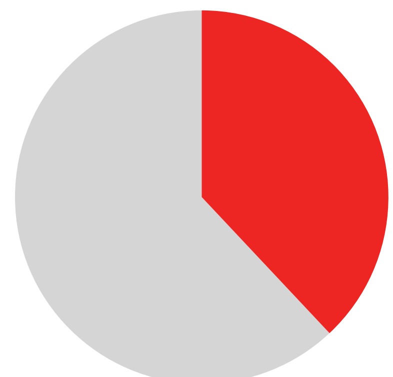
Risk managers can play a crucial role in providing clear information about campus support resources to all students and their families/caregivers. They can further support educational campaigns to decrease stigma surrounding mental health.

Promote Social Connectedness

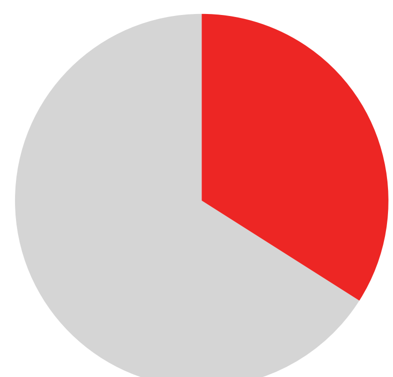
Risk managers can recommend to executive leadership that there be adequate places on campus for students to gather organically, and support campus events and activities that promote social interaction and help to develop a sense of belonging.

Good Data Is Essential

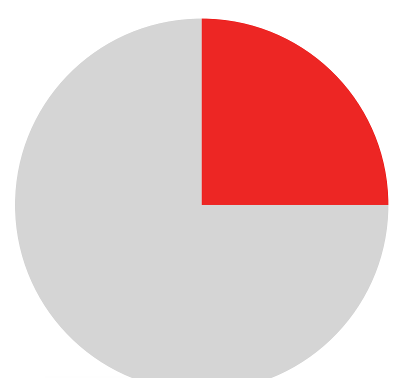
Risk managers can conduct an analysis of student mental health trends, track mental health incidents, and utilize this data to help identify patterns and inform interventions.



38%
of undergraduates experienced moderate to severe depression



34%
reported mild to severe anxiety



25%
screened positive for suicidal ideation

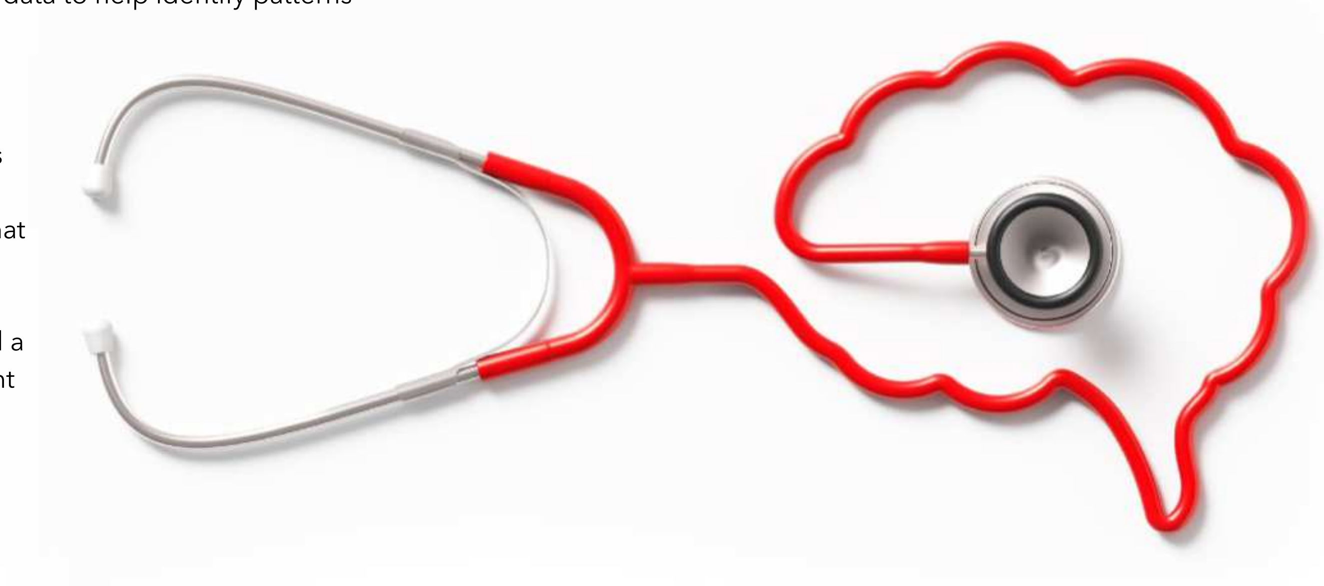
6% made a suicide plan

2.2% made a suicide attempt

2023-2024 Healthy Minds Study

BOTTOM LINE

As college students' mental health continues to be a significant concern, colleges and universities have a responsibility to ensure that there are effective policies, programs, and systems in place to support them. Risk managers are key partners in helping to lead a comprehensive approach to promote student well-being, which not only serves to mitigate risk but creates a campus culture where all students can thrive. ◆



PROPERTY COVERAGE RISK

Bradley Dlatt, Counsel, Perkins Coie LLP, has contributed to more than $100 million in insurance recoveries for policyholders nationwide. Bradley also regularly advises policyholders on complex coverage issues, including policy placements and renewals. He has experience with every major line of commercial insurance, including property and business interruption, representations and warranties (RWI), cyber general liability (CGL), directors and officers (D&O), employment practices (EPLI), and errors and omissions (E&O).

Avoiding Hidden Coverage Limitations in Property Insurance Programs

Higher education institutions are some of the world's largest landowners, with campuses and buildings sprawling across state and even national borders. Transferring the risk of loss or damage to portfolios that often include hundreds of buildings, thousands (if not millions) of acres of land, and facilities of every imaginable kind and use is, to put it lightly, complex. This is especially so in a risk landscape where natural disasters are increasing in frequency and intensity, and the costs of construction, clean-up, and remediation have never been higher.

Transferring Risk through Property Insurance

Traditionally, colleges and universities have transferred facilities and landholding-related risks through commercial property insurance programs. Evaluating which insurer or set of insurers is right for a specific institution is an iterative process that often involves intensive information exchange. Most significantly, insurers want to know the institution values of each piece of property to be insured. Institutions typically convey their valuations through a Statement of Values, which is then filed with the insurance company as part of issuing the policy.

There are several ways to calculate how a property is "valued" for insurance purposes, but that is a story for another day. What is important to know is that, amid a changing insurance market, the value of each property listed on the Statement of Values has become critically important.

- Insurers historically used the stated value of a property solely to calculate the premium charged for a specified policy and then issued policies providing "blanket" coverage across the institution's entire portfolio.
- "Blanket" coverage provides a single (often very large) aggregate limit of insurance coverage under a single insurance program that insures multiple properties.
- The alternative to "blanket" coverage is "stated value" or "valued" policies, which provide a specified limit of insurance for each individual property in a single program.

> *"Higher education institutions are best served by keeping Margin Clauses and OLLEs off their property insurance program, as these provisions are confusing and could expose your institution to unnecessary risk."*
>
> *Bradley Dlatt*

Blanket vs. Stated Value: Why This Matters

The benefit of a "blanket" program is that catastrophic losses can often exceed the stated value of a single piece of property within an extensive portfolio. It is also common for insureds to understate the value of property due to not appropriately valuing rising construction and materials costs, uncertainty over whether the insured would actually rebuild the lost property, and—to be frank—to keep premiums lower. "Blanket" limits provide some peace of mind by making the individual-stated values less critical.

The New Hidden Coverage Limitation: Margin Clauses and OLLEs

In recent years, insurers have responded to the influx of large property losses by adding new provisions that effectively seek to transform large "blanket" property programs into "stated value" insurance. These provisions are often called a "Margin Clause" or an "Occurrence Limit of Liability Endorsement (OLLE)." OLLEs, in particular, are typically drafted in confusing ways—if not outright incomprehensible—such that the average higher ed leader, or even the average risk manager, is unlikely to understand its potentially devastating effect. For example:

- **Margin Clauses** will often state that, in the event of loss or damage at an insured location, the insurer will not pay more than a specified percentage of that location's stated value listed on the Statement of Values on file with the insurer. Percentages often range from 100% to 125%.
- **OLLEs** often look something like this:

  It is understood and agreed that the following terms and conditions apply to this policy:

  1. [Language amending the definition of "occurrence"]
  2. In the event of loss hereunder, liability of the Company shall be limited to the least of the following in any one "occurrence":
     a) The actual adjusted amount of the loss, less applicable deductibles;
     b) 100% of the individually stated value for each scheduled item of property insured at the location which had the loss as shown on the latest Statement of Values on file with this Company, less applicable deductibles. If no value is shown for a scheduled item, then there is no coverage for that item; or
     c) The Limit of Liability or Sublimit of Insurance as shown on the Declarations page of this policy or as endorsed to this policy to apply to any particular insured loss or coverage or location.

Margin Clauses and OLLEs May Not Be Enforceable, but Avoid Them Anyway

While insurers have claimed the effect of these provisions is obvious to the average person, courts have not agreed. For example, the Napa County Superior Court in *Calistoga Ranch Owner, LLC, et al. v. AIG Specialty Insurance Company, et al.*, Case No. 21CV001530, ruled in 2023 that OLLEs issued by five excess insurance companies participating in a $100 million "blanket" insurance program were unenforceable. The court determined that the OLLEs violated California law—which requires that policy provisions that limit coverage must be "conspicuous, plain, and clear"—because it was neither "plain" nor "clear" to the average person that these endorsements were intended to amend the "blanket" limits stated on the face of the program.

BOTTOM LINE

Though the *Calistoga Ranch* ruling is encouraging, higher education institutions are best served by keeping Margin Clauses and OLLEs off their property insurance program, as these provisions are confusing and could expose your institution to unnecessary risk. ◆

AI RISK

Dirce Hernandez currently works as a seasoned Cybersecurity GRC Leader in the FinTech and Financial Services sector. He has over 17 years of experience spanning across Information and Cyber Security, Cyber Threat Risk Management, Cybersecurity IT Audit, and Cyber Security Research in various industries, specifically Texas State government, higher education, healthcare and financial sectors. Dirce holds both a bachelor's degree in Computer Information Systems and E-Commerce, and a master's degree in Information Security and Information Assurance Management from Our Lady of the Lake University. He holds the following industry certifications: Associate, C|CISO, CISA, CISM, CRISC, CPDSE, CSX. In addition to his professional career, Dirce is involved with higher education in a professor capacity teaching Organizational Leadership, Cybersecurity, and general IT courses for several colleges and universities. He was also a contributor for the new and updated CCSK certification v.5 exam that went live in August 2024. Dirce also served on the San Antonio ISACA leadership board from 2018-2021 and has been quoted in local and world-renowned news outlets such as *Bloomberg News* and the *San Antonio Business Journal*.

Bridging AI Innovation with AI Governance

As AI rapidly reshapes the academic landscape—from research and teaching to admissions and student support—higher education leaders face a critical dual mandate: drive innovation while ensuring responsible oversight.

Many institutions embrace AI tools, yet lag in establishing governance structures that safeguard against bias, protect data privacy, and uphold accountability. Bridging AI innovation with governance requires leadership to champion cross-disciplinary oversight, embed ethical standards in procurement and deployment, and equip faculty and staff to manage emerging risks. This balance doesn't stifle progress—it sustains it.

In the last few years, I have contributed to efforts in cloud security and AI by providing guidance and best practices for deploying AI for non-profit organizations. This article presents a strategic framework for institutions to enhance AI readiness, governance, and innovation in higher education.

AI Governance: A Pragmatic, Risk-Informed Approach

As colleges and universities strive to innovate, the Cloud Security Alliance (CSA), an organization that helps secure AI deployments through guidance, tools, and resources, emphasizes that a measured, risk-informed approach can help avoid pitfalls of compliance shortcuts or ethical oversights. Failure to incorporate risk-based strategies can lead to significant legal, operational, and reputational risks. The CSA approach advocates for proactive governance and compliance, focusing on agile frameworks that adapt to rapid technological and regulatory changes.

By integrating these strategies, institutions can avoid panic-driven responses and ensure responsible AI deployment. Institutions should also engage in continuous monitoring and support adaptive governance rather than treat risk assessment as a one-time static or set-it-and-forget process.

Further, balancing AI with robust governance structures can mitigate significant risks such as biased outcomes, privacy breaches, and AI-enabled cyber threats. Adapting governance to emerging risks maintains institutional integrity and competitive advantage.

Balancing Innovation with Security

A first step is for colleges and workforce programs to balance AI-driven agility with robust data security practices. Establishing standardized processes for data collection, cleansing, labeling, and storage is crucial to mitigate risks such as data breaches or algorithmic biases. Institutions like Miami Dade College, which recently implemented AI-driven analytics for student success, underscored the necessity of identifying and rigorous testing of security controls to prevent vulnerabilities and biases.

Recognizing AI Bias

Unchecked AI deployment can also exacerbate implicit biases, compromise data security, and introduce ethical challenges. For example, AI-generated content used uncritically in educational contexts can perpetuate harmful biases, mislead decision-making, and amplify cybersecurity vulnerabilities. Shadow AI use—unauthorized AI tools or models implemented without oversight—poses additional risks by undermining governance frameworks and compromising data security and privacy. The Cloud Security Alliance highlights these dangers, emphasizing the critical need for comprehensive governance and literacy across all institutional levels to safeguard against exploitation and malicious use.

Roles, Responsibilities, and Ethical Alignment

Accountability is foundational to successful AI governance. Institutions must explicitly delineate roles among IT, faculty, workforce training coordinators, university staff, risk and compliance officers, and business leaders. Ethical alignment, which includes fairness, transparency, and explainability, should be embedded across these roles and aligned with institutional AI deployments with evolving regulatory expectations and best practices. I will share insights into these components below:

Transparency and Explainability

AI systems inform critical decisions in education and workforce training. Transparency, through explainable AI (XAI) models and traceable decision logs, is non-negotiable. For example, the Community College of Allegheny County integrated explainable AI tools into workforce programs, ensuring transparent decisions for student certifications. The University of Texas at San Antonio's College of AI, Cyber and Computing and its Cohort for AI Responsibility Lab emphasize XAI principles, teaching students to interpret and validate AI decisions while preparing them for careers in AI-related industries.

Continuous Improvement and Adaptation

AI systems require continuous model retraining, monitoring, and evaluation. Institutions must conduct audits to adapt governance frameworks to shift technological capabilities and regulatory landscapes. Institutions should also implement regular evaluations of AI literacy among faculty and workforce specialists, ensuring their competencies remain current.

Cross-Functional Collaboration Drives Success

AI governance also requires cross-functional committees beyond technical teams. Collaborative approaches improve institutional alignment and reduce blind spots. Further, programs such as "AI Champions," a dedicated cross-collaborative task force that can be created in any organization, can discuss AI initiatives happening in their respective departments and business units. This program can be an example on how inclusive governance structures enhance AI deployment effectiveness and risk mitigation.

Metrics for Accountability

Establishing clear governance metrics—such as model performance, bias detection, security incident tracking, and compliance adherence—creates actionable feedback loops for institutions. Dallas County Community College District used these metrics to adjust their workforce AI tools while maintaining regulatory compliance. It also developed its AI Essentials course within its Web3 certification program to demonstrate practical AI application and improve student employment outcomes in AI-powered careers. ◆

"Adapting governance to emerging risks maintains institutional integrity and competitive advantage."

Dirce Hernandez

KEY TAKEAWAYS

To enhance AI readiness, governance, and ethical use, educational institutions should:

- Conduct targeted AI literacy training focused on fundamental technical understanding, ethical deployment, and critical evaluation skills.
- Establish clear governance structures defining roles, responsibilities, and accountability.
- Regularly provide hands-on, controlled experiences with AI tools to faculty, staff, and students.
- Implement continuous monitoring and periodic audits of AI systems to identify biases, compliance issues, or security vulnerabilities.
- Create institution-wide ethical guidelines to govern AI use transparently and responsibly.

By prioritizing AI governance and AI literacy, institutions can effectively bridge technological advancements and human understanding, creating secure, equitable, and innovative learning environments that prepare students for success in an AI-driven workforce.

- Cloud Security Alliance. (2024). AI organizational responsibilities: Governance, risk management, compliance, and cultural aspects. https://cloudsecurityalliance.org/artifacts/ai-organizational-responsibilities-governance-risk-management-compliance-and-cultural-aspects
- Cloud Security Alliance. (2024). AI risk management: Thinking beyond regulatory boundaries. https://cloudsecurityalliance.org/artifacts/ai-risk-management-thinking-beyond-regulatory-boundaries
- Cloud Security Alliance. (2024). AI organizational responsibilities: Governance, risk management, compliance, and cultural aspects. https://cloudsecurityalliance.org/artifacts/ai-organizational-responsibilities-governance-risk-management-compliance-and-cultural-aspects
- Cloud Security Alliance. (2025). AI security and governance. https://cloudsecurityalliance.org/articles/ai-security-and-governance
- Cloud Security Alliance. (2024). AI risk management: Thinking beyond regulatory boundaries. https://cloudsecurityalliance.org/artifacts/ai-risk-management-thinking-beyond-regulatory-boundaries
- Explainable Artificial Intelligence in Education. https://www.sciencedirect.com/science/article/pii/S2666920X22000297
- Miami Dade College Adopts AI to Improve Education and Optimize Business Operations https://edtechmagazine.com/higher/article/2024/12/miami-dade-college-adopts-ai-improve-education-and-optimize-business-operations
- Explainable AI: A Must for Higher Education https://www.linkedin.com/pulse/explainable-ai-must-higher-education-thomas-conway-ph-d--mpsrc/
- AI Machine Learning Boot Camp https://www.ccac.edu/workforce-and-community/workforce-development/ai-machine-learning-boot-camp.php
- AI Essentials: Demystifying AI and Blockchain https://web3.dallascollege.edu/courses/ai-essentials/
- UTSA's Cohort for for AI Responsibility https://careonline.github.io/
- UTSA announces College of AI, Cyber and Computing https://www.utsa.edu/today/2024/12/story/utsa-announces-college-of-ai-cyber-and-computing.html

James Geisler, PhD, NCC, LPC is the Executive Director of Wellness Services at Sacred Heart University, where his clinical work began in 2013. He is the author of *Thrive Year One: The Essential Mental Health Workbook for First-Year College Students,* a resource designed to support students in navigating the challenges of their transition to college. A passionate advocate for student and family success, Dr. Geisler is recognized for his innovative approach to mental health in higher education, shaping initiatives and policies that elevate student well-being.

Breaking the Isolation: How the "Lonely at the Top" Myth Hurts Higher Ed Leaders

Any professional familiar with the transition to, or stability in, leadership roles has likely been told at some point in their career that it's "lonely at the top." This adage, often used as a rite of passage when roles that require great responsibility and oversight are taken, has become ingrained in our society. However, with greater research and attention on the profound impact of loneliness on mental health, it is crucial to explore how this narrative shapes the experiences and internal beliefs of our institutional leaders. Does the widespread acceptance of this narrative act as a blind spot that hinders our ability to make decisions and contribute to our overall effectiveness as leaders? More importantly, does it discourage leaders from seeking necessary support to contribute positively to their own mental health and overall success in their roles?

The Risk Management and Well-Being Connection

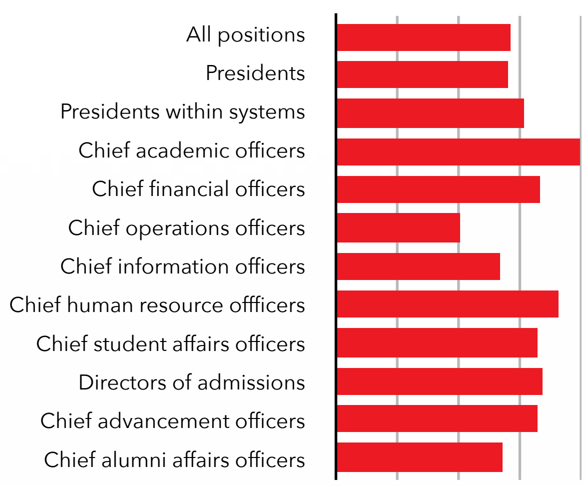
When we think about risk management in higher education, our thoughts often gravitate towards financial or operational realms and seldom the well-being of leadership. Take for example those overseeing student mental health in higher education—executives, deans, and directors of counseling and health and wellness. Their responsibilities not only involve overseeing student mental health, but they also include managing crises, ensuring campus safety, navigating hospital systems, and supporting front-line clinical staff. Yet, they are rarely asked, "Who is checking in on *you*?"

One of the greatest challenges these leaders face is being stuck in a reactive cycle of continuously responding to campus mental health issues without the opportunity to step back to address the underlying issues driving the ongoing demand for services. This is particularly challenging with leaders who lack administrative infrastructure in their wellness departments, which is an unfortunate reality for many college campuses.

As these leaders continue to encounter crises, engage in safety planning efforts, respond to the faculty and staff's concerns for students, and juggle scheduling challenges, their ability to make decisions may become increasingly reactionary and emotionally driven. Over time, this can impact their ability to engage in cross-collaboration, actively listen, and engage in strategic problem-solving, thus intensifying existing feelings of isolation or loneliness.

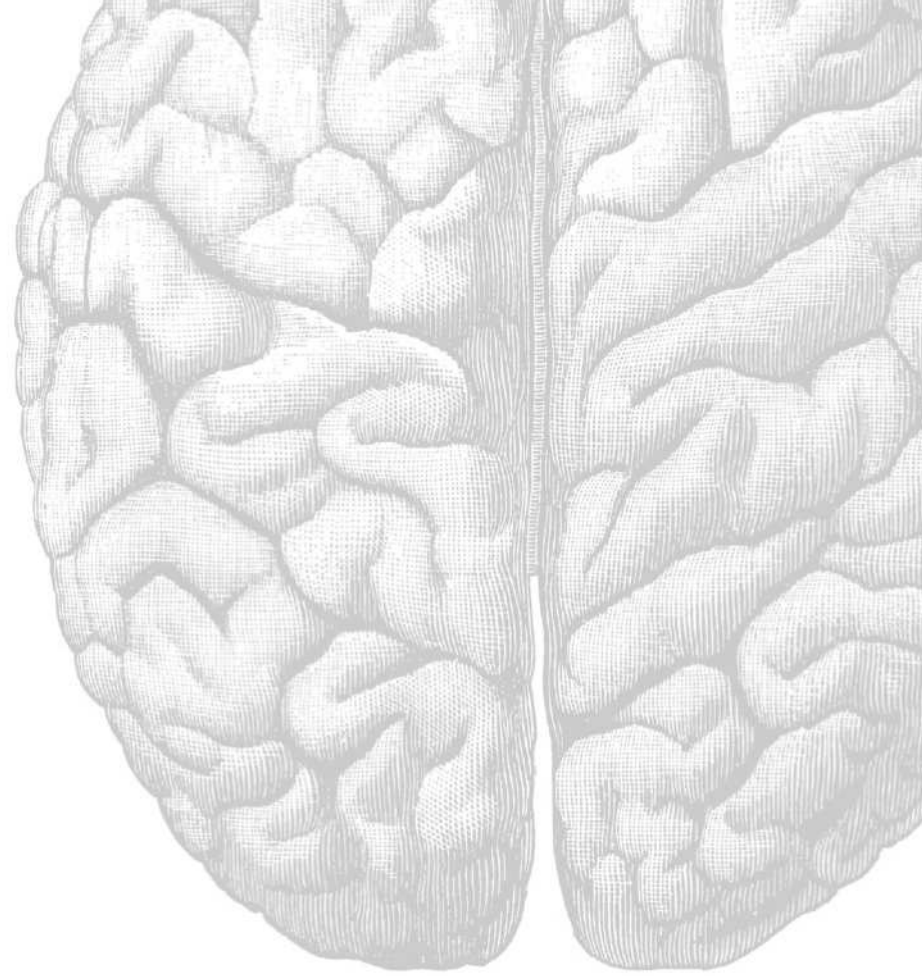
The weight of their decisions–often time-sensitive and involving multiple stakeholders–can be lonely and overwhelming. The questions become: Does it have to be lonely? What choices do these leaders have in freeing themselves from the narratives accompanying their roles?

AVERAGE TURNOVER RATES IN TOP LEADERSHIP ROLES OVER THE PAST DECADE HIT AN UNPRECEDENTED HIGH OF 21.4%



Source: Higher Education Publications, Inc, 'Turnover in top higher education administrators 2014-2024," 2024.

https://www2.deloitte.com/us/en/insights/industry/public-sector/2025-us-higher-education-trends.html



"Their responsibilities not only involve overseeing student mental health; they also include managing crises, ensuring campus safety, navigating hospital systems, and supporting front-line clinical staff. Yet, they are rarely asked, ***'Who is checking in on you?'****"*

James Geisler

Practical Strategies to Mitigate Mental Health Risk

To reduce risk and to counteract the feelings associated with the "lonely at the top" narrative, higher education leaders can benefit from:

CULTIVATING SOCIAL NETWORKS (in-person or broader, virtual networks) or seeking mentorship opportunities.

CREATING CONSORTIUMS that connect leaders in similar positions to foster environments that promote vulnerability and offer opportunities to seek multiple perspectives.

ENGAGING IN PROFESSIONAL LEADERSHIP DEVELOPMENT opportunities that focus on topics such as resilience and emotional intelligence.

ASSESSING CURRENT ADMINISTRATIVE INFRASTRUCTURE and identifying how infrastructure changes could promote positive mental health among leaders and, inevitably, future decision-making.

Tools for Decision-Making Under Pressure

In addition, higher education leaders may wonder what tools they can leverage to promote and foster sound decision-making amid times of great pressure and demand. One strategy is to utilize ethical decision-making models that offer structured support during complex experiences. A personal favorite is Forester-Miller and Davis' (2016)[14] ethical decision-making model, which, while targeted toward mental health counselors specifically, can easily be adapted to many leaders in higher education. Additionally, creating open communication with university administration about isolation-driven risks might create not only an awareness of the unique challenges of leaders, but also contribute to a shared experience among others that would warrant more supportive measures, inevitably trickling down to more effective mental health risk management.

BOTTOM LINE

Prioritizing ourselves as leaders is often done outside work hours, yet the strongest feelings of isolation can happen during the workday. Leaders should think critically about ways to invest in their mental health throughout their daily routine to manage stress and create clarity in their ability to make sound decisions. These small efforts accumulate and serve as a buffer to the often unpredictable demands of their jobs. By prioritizing both intentional wellness efforts and utilizing ethical decision-making models, leaders in higher education institutions can begin to mitigate risk and increase institutional resiliency.

Further, when leaders recognize the choices they have in shaping their narratives around loneliness and leadership, they become empowered to take control over their well-being, cultivate relationships and deeper connections, strengthen the quality of their decisions, and create a systems-level change that allows for fulfillment in their work and a stronger foundation for the next generation of leaders. ◆

14. https://www.counseling.org/docs/default-source/ethics/practioner-39-s-guide-to-ethical-decision-making.pdf

CHARTING UNPREDICTABLE CHANGE

Navigating your campus through disruption

The Growing Education Divide

University presidents were asked about the growing education divide and the U.S. electorate:

64% say they're highly concerned about the growing divide's impact on American democracy

45% say their institution has updated its campus speech policy or policies within the last 18 months

25% say they're very or extremely concerned about its implications for their institution

3% think higher education has been highly effective at responding to this divide

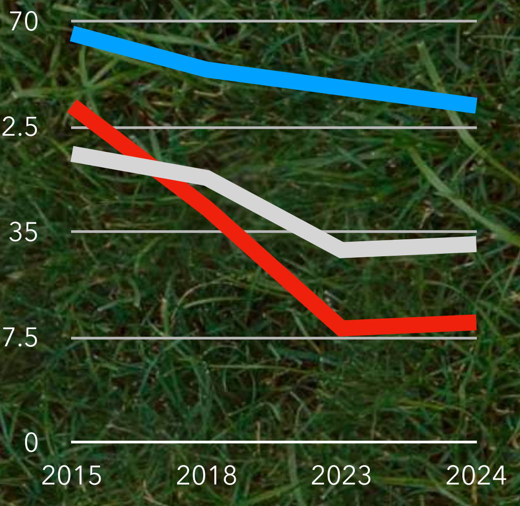
Presidents most attribute declining public confidence in higher education to concerns about the value of a college education and/or whether college is worth it. Only a fraction of presidents (15%) consider this concern to be highly valid. At the same time, a mere 1% think higher education has been highly effective at responding to declining public confidence.

Source: https://www.insidehighered.com/reports/2025/02/25/2025-survey-college-and-university-presidents

Political affiliation and views on higher education institutions

Democrat   Independent   Republican

Gallup: Share with a "great deal/quite a lot" of confidence in higher education, by political party

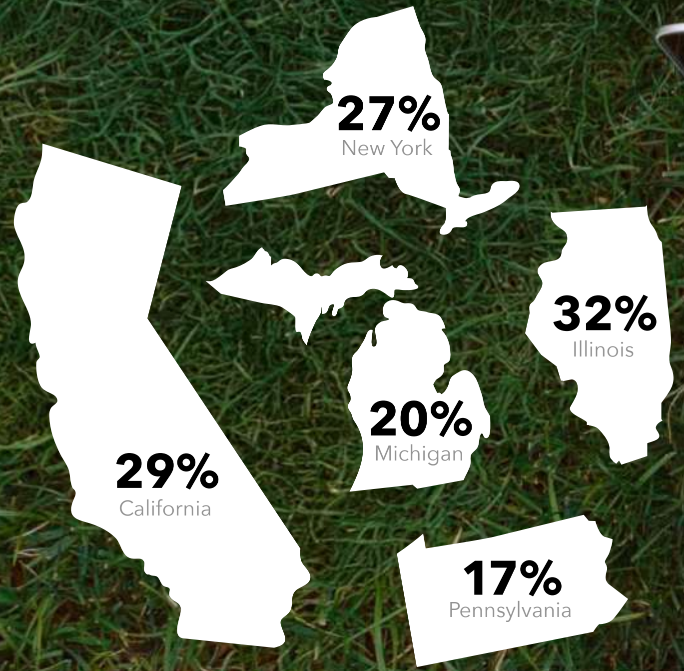


Pew: Share of Republicans that consider the impact of colleges and universities on the country positive

Source: The Burning Glass Institute authors' calculations using Gallup and Pew Research Center data.

Demographic shifts

Declining numbers of high school graduates through 2041 are projected to be most severe in places where fertility rates have been generally lower and to which fewer families have moved. As such, 38 states will see declines, with several higher than the national average:



Source (per Western Interstate Commission for Higher Education): https://www.npr.org/2025/01/08/nx-s1-5246200/demographic-cliff-fewer-college-students-mean-fewer-graduates

"This work leads me to desire **three wishes** for higher education leaders in 2025, namely that they:

Be disposed to accepting the **facts**.

Be willing to explore all **strategic options**.

Be agreeable to accepting **external help**."

Ricardo Aziz, Augusta University and principal at Strategic Partnerships in Higher Education, or SPH, Consulting Group

Source: https://www.highereddive.com/news/college-leaders-navigate-closures-mergers-2025/740280/

Rating Agencies view of Higher Education

1 S&P Global split its 2025 ratings for higher education, issuing a negative outlook for resource-constrained regional institutions while providing a stable forecast for institutions with more robust, diversified revenue streams and a broader market area.

Their outlook noted the demographic pressures facing institutions, along with challenges of meeting salary and benefit costs while also maintaining affordability.

2 Moody's, meanwhile, issued a stable outlook for higher education.

They concluded that college balance sheets will be aided by lower inflation rates and growth in net tuition revenue, philanthropic support, and state appropriations, while also recognizing demographic realities.

3 Fitch's outlook was the least optimistic of the three ratings agencies, with a "deteriorating" forecast for 2025.

Fitch analysts pointed to demographic challenges, greater market competition, "modest at best" revenue growth, and tighter state budgets as collectively confronting colleges and universities in the year ahead.

Mental Health Disconnect?

Most presidents think they are doing a good job, yet this risk remains a top risk of higher education.

81% of presidents say their institution is doing a good or excellent job promoting student health and wellness in multiple areas, including mental health.

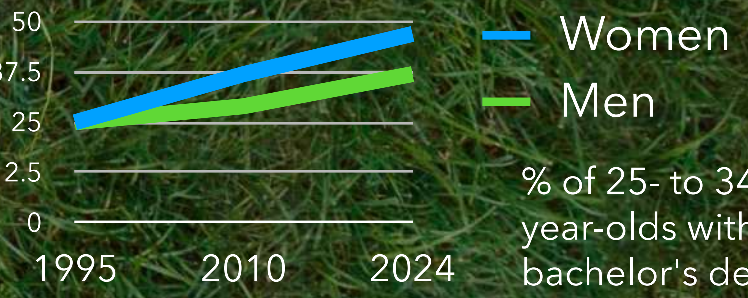
69% of presidents somewhat or strongly agree that their institution has been effective in addressing the "student mental health crisis."

44% of presidents at least somewhat agree that undergraduate mental health at their institution seems to be improving.

2025 Survey of College and University Presidents- Inside Higher Ed and Hanover Research
https://www.insidehighered.com/reports/2025/02/25/2025-survey-college-and-university-presidents

Women vs. Men in Higher Education

U.S. women have outpaced men in bachelor's degree completion for decades



% of 25- to 34-year-olds with a bachelor's degree

Source: https://www.pewresearch.org/short-reads/2024/11/18/us-women-are-outpacing-men-in-college-completion-including-in-every-major-racial-and-ethnic-group/sr_24-11-18_college-gender-gap_1/

19% Howard, one of the most elite historically Black colleges and universities in the nation, is only 25% men – 19% Black men.

Source: https://www.nytimes.com/2025/03/30/us/black-men.html

COMPLIANCE RISK

PCI Compliance Reduces Risk in Complex Campus Environments

Heather Richmond is a seasoned change agent with over 25 years of EdTech experience specializing in innovative software solutions tailored for the business of higher education. Heather has held executive positions in prominent companies focused on higher education payments technology and alumni fundraising and engagement. Currently, she is a Senior Vice President at GradGuard, helping to shape emerging strategies to help schools design policies and programs that reduce financial risks caused by third-parties such as students, vendors, and visitors.

Managing payments in higher education can feel like running a small city. Today's campuses include various merchants, numerous payment points, and multiple methods and channels through which money moves. From dining halls and athletic departments to student groups, campus clubs, and special events, the type and frequency of payments present a unique challenge for ensuring compliance with Payment Card Industry (PCI) standards.

This diverse payment ecosystem means that payment risks aren't confined to a single area of campus, but are dispersed across multiple touchpoints. Further, the frequency of these transactions makes managing compliance complex. Evaluating risk at every point where money flows is no longer optional; it's a requirement. Understanding PCI compliance helps avoid fines, prevent data breaches, and reduce reputational risk.

1,780
data breach incidents in higher education in 2024

1,537
of these involved confirmed data disclosure

System Intrusion Social Engineering & Miscellaneous Errors
made up **90%** of breaches

98% FINANCIAL motives

2% ESPIONAGE motives

Source: Verizon 2024 Data Breach Investigations Report

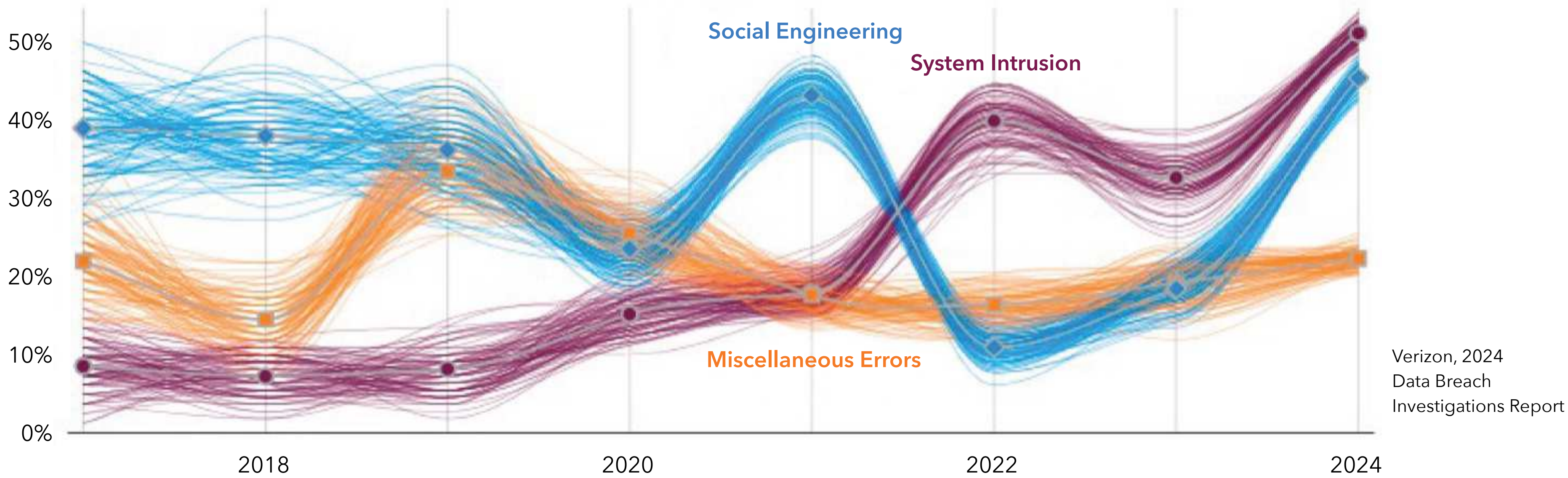
What is PCI Compliance?
The Payment Card Industry created the Payment Card Industry Security Standards Council (PCI SSC) to establish and enforce security standards for payment card transactions. Their intent was to safeguard sensitive cardholder data and mitigate fraud risks. PCI compliance is not optional. Any institution, or "merchant," that processes, stores, or transmits credit or debit card data is required to meet PCI standards.

The importance of compliance cannot be underscored, as failure to comply can result in severe penalties and increased security risks.

PCI Compliance: A Campus-wide Initiative
Ensuring PCI compliance is no longer the responsibility of a single department. It requires a campus-wide approach to effectively secure payment systems. Many campuses establish cross-functional committees that include stakeholders from the business office, data privacy, risk management, and IT security to help drive a comprehensive strategy to enhance compliance and mitigate legal and compliance risk.

Remember, the institution is the "merchant of record," which means it is ultimately responsible for ensuring PCI compliance, regardless if third-party vendors are utilized in payment processing. Universities must oversee not only their internal operations but also the payment systems and practices of any external vendors that handle cardholder data. Following are practical steps to help navigate PCI compliance across campus.

Top Patterns in Educational Services Industry Breaches[15]



Step 1: Defining the Cardholder Data Environment (CDE)

The first step in ensuring PCI compliance is understanding and defining your CDE. This includes anywhere a transaction takes place, whether in person, online, over the phone, or via a mobile device. By identifying all locations and methods where cardholder data is stored, processed, or transmitted, institutions can assess risk and develop strategies to reduce exposure.

Step 2: Reducing the CDE Footprint

A best practice is to reduce the CDE footprint by implementing a unified payment system across campus. A streamlined payment system can significantly reduce the risk of breaches and simplify the compliance process. When a unified system is in place, institutions may only need to complete a single Self-Assessment Questionnaire (SAQ) rather than multiple, thus minimizing administrative burden and reducing the risk of non-compliance.

Step 3: Identifying and Vetting Vendors

Colleges and universities often rely on third-party vendors to manage payment systems which could lead to increased risks. It is essential that these vendors meet the necessary compliance requirements to protect cardholder data, including providing PCI Attestation of Compliance (AoC) documentation. While a vendor's System and Organization Controls (SOC) report is not required to comply with PCI, it is a best practice to also require this for vendors handling large volumes of sensitive data or involved in payment processing. Strong contract language with vendors is also key to mitigating risks. It is imperative to ensure indemnification and Limitations of Liability are addressed comprehensively.

To effectively manage vendor compliance, a best practice is to store compliance documentation in a centralized location that is accessible to key departments across campus. This ensures that all parties are aware of the vendor's compliance status and can make informed decisions regarding the risk associated with their payment solutions.

From an insurance standpoint, while cyber liability insurance provides the university with coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with PCI, a university's goal should be to preserve their limits of insurance by having a robust PCI compliance program.

Step 4: Annual Assessments and Training

PCI compliance is not a one-time effort. Annual risk assessments and ongoing training are integral to maintaining compliance. Institutions should also conduct regular self-assessments to evaluate their PCI status and identify areas for improvement.

In addition to assessments, annual training for staff involved in payment processes is essential. Employees must understand PCI requirements, and their role in protecting payment data is crucial to mitigating compliance risk. Institutions can bolster compliance awareness by attending PCI conferences, participating in webinars, or adopting a "train the trainer" approach to enhance institutional expertise and foster a culture of security where everyone is encouraged to put on their risk management hat!

Step 5: Navigating the PCI DSS v4.0 Update

As of March 31, 2025, the PCI DSS v4.0 requirements were fully implemented, bringing with them significant changes. This update includes more than 50 new requirements, which will apply to all merchants, including higher education institutions. Additionally, the Self-Assessment Questionnaire format has been updated to reflect these changes, and institutions must adjust their compliance processes accordingly.

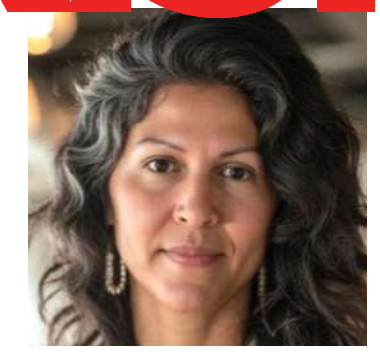
You can stay informed about these updates through the PCI Security Standards Council's resource hub[16] which offers valuable information for understanding the new requirements.

CONCLUSION: A PROACTIVE APPROACH TO CAMPUS PAYMENT SECURITY

Maintaining PCI compliance is not just about meeting standards; it's about safeguarding your institution's reputation and reducing the risk of costly data breaches. With payments occurring across hundreds of touchpoints on campus, managing compliance can be a challenge. However, by adopting a proactive, cross-functional approach which includes regular risk assessments, training, enhanced vendor oversight, and centralized systems, institutions can better navigate this complex landscape and foster a more secure payment environment for their students, staff, and visitors. ◆

15. Verizon, 2024 Data Breach Investigations Report: http://verizon.com/dbir
16. https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub

ENTERPRISE RISK



Melissa Diaz is the Director of Risk Management at the University of San Francisco (USF) and also oversees the Environmental Health and Safety department. Melissa has been the Program Administrator for the Jesuits West Insurance Group Consortium (JWIG) for the last 3 years, providing leadership to the group's five core members. Prior to joining USF, Melissa worked in the Public Entity Group at Alliant Insurance Services and has over 23 years of risk management and insurance experience. Melissa holds an Associate in Risk Management (ARM) and MBA from the University of San Francisco.

On the 2025 Board Agenda: Enterprise Risk Management (ERM)

One of the primary responsibilities of a board member or leader at an institution of higher education is effectively overseeing institutional risk. With the new administration in 2025 and its potential to create new risks and amplify existing risks, it is important now more than ever to be proactive and look at risk management holistically. But how?

Why Boards and Executives Should Support ERM

Enterprise Risk Management (ERM) allows an institution to proactively identify, assess, monitor, and prioritize risks that can affect the institution's objectives. ERM allows for risk-informed decision-making, increased transparency, and greater governance that supports an institution's goals and objectives. Engaging the board with mission-critical risks through an ERM program should be at the top of every institution's agenda this year. According to the *RIMS State of ERM Report*, "Organizations with formalized ERM programs perform better than organizations without formalized ERM programs." As the world begins to move ahead, facing major political, geopolitical, and social challenges, traditional risk management (or "siloed risk management") will no longer be enough.

Emerging Risks in 2025

The following risks require a proactive and enterprise approach; and by relying on traditional siloed risk management, there may be blind spots.

- Diversity, Equity, and Inclusion (DEI) programming investigations and crackdowns
- Sex and gender identity, especially in athletics
- Federal funding freeze concerns on grants, loans, and research
- Targeted investigations under the False Claims Act
- Immigration and international travel changes
- Free Speech and the First Amendment
- Pivot away from sustainability initiatives

A Roadmap to ERM

In 2024, the American Institute of Certified Public Accountants-Chartered Institute of Management Accountants (AICPA-CIMA) 2024 *State of Risk Oversight Report* surveyed a range of organizations in which 37% reported having a formal ERM process in place, and 34% did not have an enterprise-wide view of risk[17]. This is an improvement in the engagement levels of companies adopting formal ERM programs since AICPA's 2015 *State of Risk Oversight Report*, where only 25% of organizations reported having a formal ERM process in place[18].

Many institutions do not know where to start an ERM program, and even experienced risk professionals struggle to find where to begin. The following insights can help institutions build a successful ERM program:

- **Leadership & board buy-in and support**: Build the case for ERM to the board of directors and senior administration. As higher education leaders, you set the tone for the organization's risk culture and, ultimately, the ERM program. Board involvement, leadership, and oversight are essential for the success of ERM. This responsibility may fall within the Audit Committee.

- **Alignment with strategic plan and objectives**: Create an ERM mission/vision statement that aligns with the strategic plan, environment, and culture. Reflect on the institution's short-, mid-, and long-term objectives. A helpful resource is the International Organization for Standardization (ISO) 31000 framework[19], which defines risk as, "the effect of uncertainty on objectives." Depending on which ERM framework your institution utilizes to leverage your program, such as ISO 31000 or the Committee of Sponsoring Organizations of the Treadway Commission (COSO), they share common themes. An ERM framework provides structure and methodology to approach risk consistently, strategically, and with accountability.
- **Build the foundation**: Who will be the ERM leader championing a risk-aware culture at your institution? Select that leader, create a plan, and define a timeline. Make sure that risk, compliance, and internal audit functions are aligned with the plan. According to the Institute of Internal Auditors' publication *Internal Audit's Role in Enterprise Risk Management*, two of the most important ways an audit can add the most value are by 1) providing objective assurance that the major business risks are being managed appropriately and 2) providing assurance that risk management and the internal control framework is operating effectively[20].
- **Governance**: At every institution, the ERM governance structure and information flow will be varied. The governance structure provides guidance on the management and roles and responsibilities of the ERM program. It is important to occasionally review the risk governance structure because the risk landscape is constantly changing.
- **Hire a consultant**: The decentralized nature of higher education can make it challenging to coordinate risk management across an institution. Consultants can help with ERM implementation from either a ground-up strategy or at tactical points in the process.
- **Demonstrate a small victory**: Your institution does not need to start with a campus-wide ERM implementation. Undergo ERM with one department, provide results to leadership, and then champion to expand the efforts campus-wide.
- **Remember, slow progress is still progress!** This is likely the case at many institutions. Timing can be everything, as noted by the impact of the pandemic on USF's ERM program.

The time has come for institutions to move beyond traditional risk management programs and embrace ERM as a strategic institutional initiative. Forward-thinking leaders who prioritize risk at the board level will better position their institutions for greater resilience and success in this era of unprecedented change. ◆

CASE STUDY:
ERM AT THE UNIVERSITY OF SAN FRANCISCO

2011
Internal audit conducted campus-wide risk assessment

2015
Internal audit conducted campus-wide risk assessment

2018
Hired consultant to assist Risk Management with ERM implementation

2019
Presentations to leadership for executive support, program design, and risk identification

2020
Presentation to Audit Committee on 2019 findings (*Program paused due to pandemic)*

2023
Audit Committee support to continue efforts

2024
Established governance structure, creation of Enterprise Risk Committee (ERC), risk assessment, prioritization, evaluation of existing controls, development of risk management/mitigation plans, Audit Committee presentation on findings

2025 & beyond
Program officially kicked off. Deployed a web-based tool for reporting purposes; monitor, measure, and report on results; embed the discipline throughout the organization; and sustain the program.

17. https://www.aicpa-cima.com/professional-insights/article/navigating-complexity-the-current-state-of-risk-management
18. https://erm.ncsu.edu/wp-content/uploads/sites/41/migrated-files/AICPA_ERM_Research_Study_2015.pdf
19. https://en.wikipedia.org/wiki/International_Organization_for_Standardization
20. https://www.theiia.org/globalassets/site/content/articles/industry-knowledge-brief/2019/internal-audits-role-in-enterprise-risk-management/iia-ps-kb---internal-audits-role-in-enterprise-risk-management.pdf

DATA PRIVACY RISK

Tom Infurna is a Vice President in Marsh's Cyber Practice, serving as a lead advisor and placement specialist for clients across the country. Based in Marsh's New York office, Tom is responsible for assisting clients with risk identification, risk mitigation, and risk transfer solutions for cyber, professional, and technology liability exposures. A significant portion of Tom's client portfolio serves education clients; and with his experience, he serves as Education Industry Specialist within Marsh's Cyber Practice. In this role,Tom works closely across the practice to support education client needs.

Tom holds a BS in Business Administration from Fordham University and is a member of the Professional Liability Underwriting Society.

Navigating Data Privacy Risk in Higher Education

In today's digital age, the value of data continues to skyrocket. The collection, analysis, sharing, and storage of data is integral to success in the day-to-day operations of any higher education institution. Yet as the opportunities of data use continue to increase, the risks associated with data continue to grow with greater financial, legal, and operational implications than ever before. In a rapidly evolving risk landscape within higher education, it is critical to prioritize protecting sensitive information through effective data risk management strategies.

Current Trends in Data Privacy Risk

1. Evolving tactics of cybersecurity threat actors

Threat actors frequently target higher education institutions with cyber-attacks due to the vast array of sensitive information that institutions manage, including student information, employee information, research data, and financial records. Since the onset of the COVID-19 pandemic in 2020, ransomware attacks have become a lucrative scheme for threat actors, and they remain a persistent threat facing higher education institutions.

In 2024, the two most common attack vectors for threat actors to gain unauthorized entry into a network were phishing and stolen or compromised login credentials[21]. Threat actors are now exploiting emerging AI technologies to make phishing attempts appear more legitimate and enable malware to mutate in real time to evade detection[22]. Following unauthorized entry into a network, the sophistication of ransomware attacks has continued to escalate. In the 4th quarter of 2024, 74% of ransomware cases involved lateral movement by a threat actor within a network. Additionally, 87% of ransomware cases involved data exfiltration, which has fueled concerns about privacy liability issues[23].

While the sophistication level of ransomware groups varies greatly, more sophisticated ransomware threat actors provide ransomware-as-a-service toolkits to less sophisticated threat actors to lower the barrier to entry to launch an attack and increase the overall volume of ransomware activity[24].

2. Dynamic privacy regulatory framework

From a regulatory perspective, a patchwork of data privacy laws now apply across many states. Beginning with the passage of the California Consumer Privacy Act (CCPA) in 2018, 19 states have enacted comprehensive privacy laws as of the end of 2024[25]. State comprehensive privacy laws, which are separate from breach notification laws, govern a host of issues such as geolocation, data collection, and biometric information. An additional 16 states have privacy legislative bills in process as of the beginning of 2025.

As the privacy regulatory landscape rapidly evolves, understanding how and where your institution uses data is crucial for compliance with applicable comprehensive privacy laws. The absence of a unified federal standard exposes higher education to further risk, making it challenging for institutions to comply with a wide range of state privacy laws across various governing jurisdictions. Collaboration with legal counsel is essential to maintain compliance in today's dynamic privacy regulatory environment.

3. Third-party vendor risks

Higher education institutions frequently engage with third-party vendors for various services, including IT management, data storage, and educational technologies. These relationships introduce additional layers of risk, as vendors may have access to sensitive institutional and student data. The MOVEit file transfer tool cyber incident in 2023, which exposed the sensitive data of many institutions, exemplified significant threats posed by third-party vendor vulnerabilities. Effective third-party risk management is therefore essential, involving thorough vetting of vendors, continuous security monitoring, and the implementation of stringent data sharing agreements to ensure that third-party partners adhere to the same rigorous data privacy standards as the institutions themselves.

"As the opportunities of data use continue to increase, the risks associated with data continue to grow with greater financial, legal, and operational implications than ever before."

Tom Infurna

How Cyber Insurance Is Responding to Data Privacy Risk

Coverage for privacy liability and regulatory proceedings is commonly included as a core component of a cyber insurance policy. While this coverage contemplates defense and liability for the unintentional violation of a privacy or cyber law, several insurers are beginning to adjust their coverage approach. In light of steady increases in the frequency and severity of privacy-related events, some cyber insurers may now seek to add policy exclusions for wrongful collection of data, particularly for higher education institutions that are connected to a healthcare system. As complex data privacy risk continues to evolve, discussing privacy liability and regulatory proceedings coverage with your insurance broker is essential. If a wrongful collection exclusion is present on your current cyber insurance policy, ask your broker about risk transfer solutions to address this exposure before your next cyber insurance renewal cycle.

Actionable Insights for Boards to Mitigate Data Privacy Risk

1. **Promote a culture of data privacy and security awareness across your institution.**
   - Establish data governance committees for clear leadership and accountability.
   - Engage key stakeholders in data privacy initiatives.
   - Provide annual cybersecurity training for faculty and staff.
   - Maintain regular cadence of phishing tests for faculty and staff.
2. **Develop and maintain comprehensive data governance frameworks.[26]**
   - Allocate financial resources for data governance leadership at the enterprise level, including designation of a Chief Data Privacy Officer.
   - Adopt institutional policies and procedures for the collection, storage, access, and disposal of data.
   - Conduct regular Privacy Impact Assessments to identify and mitigate potential privacy risks.
   - Collaborate with legal counsel to ensure compliance with evolving data privacy regulations.
3. **Implement data privacy management tools.[27]**
   - Maintain comprehensive inventory of the types of data your institution handles, including but not limited to: student data, employee data, research data, financial records, and intellectual property.
   - Classify data under appropriate categories of sensitivity, such as: public, internal, confidential, and restricted.
   - Enforce multi-factor authentication (MFA) to protect access to any systems, networks, or applications that contain sensitive information.

BOTTOM LINE

Effective data privacy risk management requires consistent support across an institution, from executive board leadership to faculty and staff. Establishing data governance leadership, investing in strong cybersecurity posture, and promoting privacy and security awareness can help your institution to manage the rapidly evolving and growing risks associated with data privacy. ◆

21. IBM Cost of a Data Breach Report 2024
22. Sentinel One 10 Cyber Security Trends For 2025
23. Coveware Quarterly Report Blog https://www.coveware.com/blog/2025/1/31/q4-report
24. Sentinel One: 10 Cyber Security Trends For 2025
25. IAPP US State Comprehensive Privacy Laws Report, 2024 Legislative Session us_state_privacy_laws_report_2024_session_overview.pdf
26. EisnerAmper Data Privacy in Higher Education
27. RiskDataControl.com The Ultimate Guide to Data Privacy Risk Management

NIL RISK

Andrew Allen works with Dissinger Reed, A Division of HUB International. Andrew specializes in NIL risk management strategy and student athlete medical insurance. Dissinger Reed works with over 300 athletic departments across the nation.

To learn more, connect with Andrew at andrew.allen@hubinternational.com.

How Will the House Settlement Transform Collegiate Athletics?

It is hard to follow collegiate sports without seeing news of the "House Settlement" and how it will transform collegiate athletics forever. The crux of the lawsuit is centered around name, image, and likeness (NIL) rights, and concerns over the exploitation of student-athletes. The full complaint can be found[28] here.

Key Points of the Settlement

When the settlement is approved, it will bring several reforms to college athletics, including:

- Direct payments from athletic departments to student-athletes: Schools can share up to a maximum of $20.5 million with their athletes. This compensation can come in the form of scholarships or NIL rights.
- Restrictions on third-party NIL agreements: If an NIL deal with an athlete comes from a source outside of the university, then it will be subject to a "Deal Clearinghouse" or Fair-Market Value (FMV) evaluation. If the deal is not deemed to meet FMV standards, then it will be denied. This is going to be a highly complex matter moving forward[29].
- Replacing scholarship limits with roster limits: The old model of college athletics had limits on scholarships that could be offered to athletes. Still, there was no limit on the number of athletes that schools could have on a roster. Athletes who were not on scholarship were called walk-ons. Post-settlement, caps[30] will be put on the number of athletes that can be on a specific roster, and every athlete will be eligible for a scholarship.

What Needs to Happen Before the Settlement is Approved?

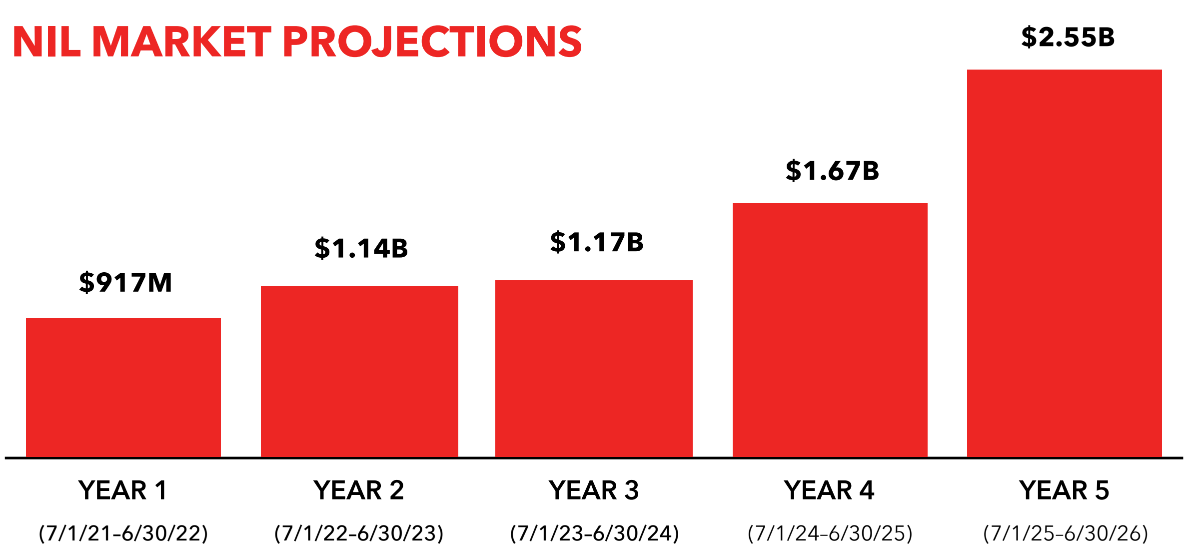
On April 7, 2025, attorneys for both sides and objectors to the settlement met in front of Judge Claudia Wilken in the Northern District of California to discuss the finalized terms and seek final approval. Judge Wilken indicated that she accepted the terms of the settlement, but two key issues still need to be addressed:

1. Roster limits: Judge Wilken felt that taking opportunities away from current athletes would be unfair. She suggested that all current athletes be grandfathered in, with new roster limits being implemented over time.

2. The effect of the settlement on future athletes: She asked that they amend the language locking in future athletes to the settlement, but rather leaving a window open for them to object to terms when they start participating in college athletics.

"The NIL market has exploded from $917 million in 2021-22 to an expected $1.67 billion in 2024-25 – with no signs of slowing down."
Opendorse

NIL MARKET PROJECTIONS



Estimated annual spend on Commercial, Collective, and Collegiate NIL products and services calculated by extrapolating primary data based on 150,000+ anonymized transactions from 100,000+ student-athletes facilitated or disclosed through Opendorse between July 1, 2021, and June 7, 2024.

Source:
https://biz.opendorse.com/wp-content/uploads/2024/07/NIL-AT-3-The-Annual-Opendorse-Report-1.pdf#gf_56

"Looking down the road, how institutions classify athletes is going to change. A model where athletes are considered employees is coming, and adding athletes as W-2 employees will have a dramatic impact on schools' workers comp, health benefits, and insurance costs."

Andrew Allen

What Does This Mean from a Risk Management Perspective?

This question is very hard to answer in the short term, even though it could have major implications for how your athletic department approaches risk. For starters, athletes will be collecting up to $20.5 million in revenue from the school, so institutions will be required to generate new revenue streams to share with athletes to mitigate financial risk.

At HUB International, we have created an insurance program that schools can use to help address the risks associated with revenue distribution, and ease the burden on alumni and supporters to fund the program year over year.

Looking down the road, how institutions classify athletes is going to change. A model where athletes are considered employees is coming, and adding athletes as W-2 employees will have a dramatic impact on schools' workers comp, health benefits, and insurance costs.

There are also going to be further legal challenges to the settlement in regards to Title IX, employment status, roster limits, and how the current settlement will affect future athletes. This will result in additional legal risks and costs.

Additional resources may also be needed to help maintain compliance. It is a good idea to be in frequent contact with your compliance team and Title IX coordinator in your athletic department.

How Do I Stay Up to Date?

Both parties are expected to be back in front of Judge Wilken in the coming months with revised terms. Athletic departments are already preparing for the settlement terms to take effect. News about the settlement seems to break every day. Here are a few helpful resources you can follow to stay up to date and prepare your institution to be compliant and resilient in times of change.

Mit Winter
x.com/WinterSportsLaw

Mit is an attorney at Kennyhertz Perry LLC in Kansas City and an expert in sports law. He was recently named one of the top 70 people in the NIL space.

Jason Belzer
x.com/JasonBelzer

Jason is the Co-founder and CEO of Student Athlete NIL (SANIL) and Co-founder of AthleticDirectorU. He is a leading voice on NIL and the business of college athletics.

Ross Dellenger
x.com/RossDellenger

Ross is a reporter for Yahoo Sports and the leading media source on the House settlement.

Jason Montgomery
www.huschblackwell.com/professionals/jason-montgomery

Jason is a former NCAA investigator and now an attorney at Husch Blackwell. He consults with many programs on NCAA compliance issues. ◆

SCAN ME

Stay informed on the House settlement here:

AthleticDirectorU
https://athleticdirectoru.com/

28. https://caselaw.findlaw.com/court/us-dis-crt-n-d-cal/2140891.html
29. https://niledu.substack.com/p/why-nils-fair-market-value-is-challenging?utm_campaign=post&utm_medium=web
30. https://sports.yahoo.com/new-college-sports-roster-limits-revealed-as-house-settlement-expands-scholarship-numbers-210542040.html

CYBER RISK

An Interview with a Chief Information Security Officer (CISO)

Priya Mouli is an accomplished Cybersecurity, Risk Management, Tech and Data Professional, and Thought Leader with ~20 years of experience in IT Strategy, Enterprise Resiliency, Privacy, Data/AI Governance, and Compliance. She is currently the Director of IT Security & Information Security Officer at Sheridan College, Ontario. Before moving to Canada, Priya spent a decade advising global financial services firms on Wall Street and technology organizations in the Bay Area. She has a commendable history of collaborating with senior leadership and the boards of companies of different sizes, risk, and compliance profiles to formulate robust and agile cyber/risk strategies and working with operational teams to implement them.

Priya has authored global publications and is frequently invited to chair and speak at conferences sharing industry insights on current and upcoming topics and spreading awareness on cyber risk and DEI topics. Priya's international experience across the US, UK, Canada, China, and India has honed her ability to work in multicultural environments by having a global mindset, working and communicating effectively with people across the globe.

SCAN ME

linkedin.com/in/priya-mouli/

Cyber risk is listed as one of the top risks facing higher education. As threat actors grow more sophisticated and regulatory requirements evolve, gaining leadership support to invest in cyber risk management is essential. Risk Management and Information Security leaders form a critical partnership to help combat risks beyond the cyber insurance renewal.

To equip boards and fiduciaries with strategies to mitigate these risks, I engaged with Priya Mouli, the Head of Information Security and Compliance at Sheridan College. She will share her insights on how IT leaders, Risk Management, and the executive sponsorship at the board level are essential to staying ahead of cyber risk.

Q1: Can you share your journey into cybersecurity? How did you transition into this field?

Pryia Mouli (PM): Sure! I am Priya Mouli, and I am the Information Security Officer at Sheridan College in Ontario, Canada. I have ~20 years of experience in cybersecurity, privacy, risk management and compliance, resiliency, data and now AI governance.

My path into cybersecurity was not linear. Graduating with an engineering degree, I started my career as a software developer. I then pursued my MBA to explore the intersection of technology and business and to challenge myself to become a subject matter professional in another domain of technology.

Subsequently, I landed roles with the Big 4 consulting firms, starting with Deloitte, where I focused on technology risk, cybersecurity, and enterprise resiliency. I have lived and worked in six countries, and my career path has taken me to support global organizations across industries in the public and private sectors, with their cyber and risk management journeys and progressing their maturity.

I am passionate about enhancing security awareness and promoting a culture of risk consciousness within organizations. I speak at global conferences and summits sharing industry insights/perspectives, spreading awareness on cyber risk and DEI topics, and authoring global thought leadership publications.

Tracey Swift (TS): I appreciate that you shared how your path into cybersecurity was not linear. I noticed a similar pattern among risk management professionals. I also like how you integrated the disciplines of cybersecurity, risk management, and enterprise resiliency in your role. In today's risk management landscape, it is essential to address risks in a holistic manner, and your career path exemplifies this evolution.

"Academic institutions are attractive targets for threat actors as they are a gold mine of sensitive data by way of PII and research data, have an ethos of open sharing, and may have low budgets earmarked towards cybersecurity and leaner teams."

Priya Mouli

Q2: One theme we emphasize in HigherEdRisk is that cross-functional collaboration plays a critical role in risk mitigation. Who do you view as strategic partners in preventing cybersecurity incidents?

PM: I would like to respond to this question by first looking at the sensitive data that higher educational institutions collect, store, and process. This includes personally identifiable information related to students and employees, institutional financial data, and research data that qualifies as Intellectual Property (IP). So I would say that building relationships across the institution starting with the rest of IT, Risk Management, and other administrative departments (such as Finance, Human Resources, Legal, Communications, and Faculty departments besides Research) are key.

It is important to build these partners and allies beyond IT as "cybersecurity is a team sport." I have built good relationships across the institution by making cyber security and cyber safe practices easy and consumable for our community members. I have further brought in institution-wide stakeholders and kept them involved in the cyber journey.

Some examples include Sheridan College building our IT Security Roadmap in early 2024 and socializing this across the institution including administrative units and academic/faculty departments as above, while actively involving these stakeholders and soliciting their feedback. I also conducted our first cyber tabletop exercises last year for the technical/operations and executive teams to be able to build the muscle memory of who does what and when in moments of crisis.

TS: Thanks for sharing that cybersecurity is a team sport. We have a similar saying in risk management that "we are all risk managers." This inclusive approach encourages diverse perspectives to help mitigate cyber risk.

Q3: In your opinion, what are the top three cybersecurity risks in higher education?

I would say that the top three cyber risks are social engineering attacks by way of phishing; network, system, and application-vulnerabilities; and denial of service (DoS) attacks.

PM: All of these risks can result in ransomware and data breaches/leakage, like in any other industry. These are also the top cyber risks due to the unique environment and the nature of operations in post-secondary institutions. For example:

- having a complex IT infrastructure;
- using legacy systems;
- handling a vast amount of sensitive data including personally identifiable information (PII), research data, and IP; and
- having a diverse population of students, faculty, staff, alumni, contractors, international agents, and donors/patrons that can be subject to social engineering scams.

As a result, controls/measures need to be thoughtful while keeping in mind the institution's context and risk appetite.

TS: Social engineering, ransomware, and data breaches are often mentioned in the risk and insurance industry as top risks, so it's important to see that we are aligned.

Q4: When speaking with your peers, what is one tool or resource that you hear repeatedly that executive leadership, boards, and fiduciaries should invest in to help mitigate cyber risk?

PM: Having a budget or resources that allows for a dedicated security operations center (SOC) within the institution would have far-reaching benefits in helping mitigate cyber risk. Academic institutions are attractive targets for threat actors as they are a gold mine of sensitive data by way of PII and research data, have an ethos of open sharing, and may have low budgets earmarked towards cybersecurity and leaner teams.

TS: I agree. In the insurance world, higher education presents unique cyber insurance challenges due to its decentralized IT infrastructure and vast amounts of data. A dedicated SOC sounds like an ideal way to reduce risk.

"Appreciating cybersecurity as a systemic risk in academic environments, given that we are inherently digital and accordingly allocating a fairly sized budget towards cybersecurity, would go a long way."

Priya Mouli

Q5: In the higher education risk management space, we often hear that academic freedom can create barriers to implementing a strong information security program. Do you have suggestions on how to balance academic freedom and information security requirements?

PM: I believe that academic freedom and information security can co-exist. As in my response to Q2, building your partners and allies on the faculty side by demystifying cyber security measures and articulating their benefits to them would work well. Some examples that come to mind are having controls around network zoning, having multi-factor authentication (MFA), and using biometric authentication that would offer enhanced security and a seamless user experience.

TS: Biometrics is an interesting proposal. The legal and regulatory landscape around biometric data collection and storage is another area that keeps evolving, so institutions will have to remain informed on changing regulations.

Q6. Higher education typically has lower security budgets than the private sector, yet it faces similar threats. What do you feel is the one risk mitigation that, if implemented, would generate the best return on investment (ROI) in terms of keeping an institution more secure?

PM: I would say that applying protection measures focusing on digital crown jewels (i.e., critical assets) would offer the best ROI in keeping an institution secure. By critical assets, we mean systems and data that are essential for operations and those that are sensitive from a privacy and intellectual property standpoint. Employing a defense-in-depth strategy to protect these assets would go a long way—this refers to layered controls (e.g., network segmentation, application access and vulnerability management, data encryption across data at rest, in transit, etc.).

TS: Thanks for sharing these best practices. Implementing robust layered security controls can mitigate risk and help institutions secure better cyber coverage terms and lower premiums.

Q7. What themes do you see in your industry where you can use more board and fiduciary support to help create a stronger cyber risk posture?

PM: Appreciating cybersecurity as a systemic risk in academic environments, given that we are inherently digital and accordingly allocating a fairly sized budget towards cybersecurity, would go a long way. This, along with periodic involvement in tabletop exercises/cyber crisis simulations, would help enhance the risk posture and cyber event preparedness.

TS: Great takeaways, Priya. As our institutions become fundamentally digital, the exposure to increased cyber threats impacts institutional reputation and financial stability. Having boards participate in risk mitigation strategies such as crisis simulations is a great way to help build cyber risk understanding and drive strategic investment in robust cybersecurity capabilities. Together, Risk Managers and Information Security Officers can help lead that charge. Priya, thanks for your strategic insights. I am sure our readers will find them helpful. ◆

Read more about Priya's career journey and insights here:

Priya's recent CISO Award across North America

https://www.linkedin.com/posts/priya-mouli_i-am-deeply-honored-to-receive-thecisos-activity-7244793245048733697-sKeN/

Priya's story to date and of persistence

https://www.linkedin.com/posts/priya-mouli_heretostay-iwd2023-womenincyberprivacyfincrime-activity-7041767557850169344-HGWU/

Priya's recent presentation at ISACA on Gen AI

https://www.linkedin.com/posts/priya-mouli_generativeai-isacacon-genai-activity-7298393309750734849-Dm9E/

This issue's key questions:

Compliance Risk

How comprehensive is our institution's antitrust compliance program, particularly regarding our admissions, financial aid, and employee recruitment practices?	When was the last time we conducted training for key personnel to ensure they understand how to avoid potentially collusive behavior with peer institutions?	How are we ensuring cross-functional oversight of our campus-wide payment ecosystem, particularly with implementing PCI DSS v4?	What documentation must we verify that all third-party vendors handling cardholder data meet compliance requirements?

Mental Health Risk

What mechanisms have we implemented to assess leadership burnout and isolation across our institution, particularly for those in crisis-response roles, and how do we measure whether our support systems are effective?	What specific infrastructure investments can we support to help combat student mental health and leadership mental health?	What metrics do we collect to measure the effectiveness of our early identification systems, crisis response protocols, and mental health services in reducing student mental health risk?	What specific environmental safety measures have we implemented as part of our means safety protocols, and how regularly are we conducting environmental scans to identify potentially dangerous areas or access points that could be used for student self-harm?

AI Governance, Cyber Risk, and Data Privacy

What policies have we implemented to address 'shadow AI' usage across campus?	How are we balancing our innovation initiatives with appropriate risk-informed safeguards for data privacy, security, and algorithmic bias?	How are we measuring the effectiveness of our governance framework against specific metrics such as model performance, bias detection, and security incidents?	How frequently do we conduct cybersecurity tabletop exercises that include leadership and board members?

What specific insights from these simulations have been incorporated into our institution's security roadmap and budget allocations?	Have we implemented a defense-in-depth strategy that specifically protects our institution's 'digital crown jewels', and do we have clear metrics to demonstrate the effectiveness of our controls?	Has our institution established a data governance committee with clear leadership accountability?	Do we have an enterprise-level Chief Data Privacy Officer with adequate resources to maintain a comprehensive data inventory and classification system across all our departments?	Do we have a formalized third-party vendor risk management program?

Enterprise Risk Management (ERM)

How effectively is our current risk governance structure equipped to address the emerging risks identified for 2025, such as federal funding concerns, free speech, and NIL?	Has our institution implemented a formal ERM program? If not, why?	Do we align our risk management framework with our strategic plan?

Insurance Coverage Limitations

Has our institution recently reviewed our property insurance policies specifically for the presence of Margin Clauses or Occurrence Limit of Liability Endorsements (OLLEs); and if these clauses exist, what strategy is in place to eliminate them during our next renewal?	How accurate is our Statement of Values for campus properties? Does it adequately reflect current construction costs and replacement values to ensure we're not underinsured if our policy includes limitations based on stated values?	Do our cyber insurance policies contain any exclusions for wrongful data collection that could leave us with significant uninsured exposure?

Name, Image, Likeness (NIL)

How will implementing direct payments to student-athletes and roster limits impact our institution's financial strategy?	What steps will leadership take to ensure compliance with the evolving NIL regulations and the anticipated legal risks?	Given the potential for future legal challenges regarding Title IX and athletes' employment status, how will leadership adapt the institution's risk management and insurance strategies to address the changing landscape of collegiate athletics?

Have a suggestion or would like to contribute? E-mail tswift@higheredrisk.com today. Stay in touch via **LinkedIn** and subscribe to be sure not to miss the September issue.

linkedin.com/company/higheredrisk/

SCAN ME

HigherEdRisk

HigherEdRisk

3219 E. Camelback Road #786
Phoenix, AZ 85018

NACUA 2025 Annual Conference
National Association of College and University Attorneys
June 22-25, 2025
Seattle, WA

ACUHO-I LIVE! 2025
Association of College and University Housing Officers-International
June 28-July 1, 2025
Columbus, OH

70th SHEEO Annual Meeting
State Higher Education Executive Officers Association
July 14-17, 2025
Washington, D.C.

UNCF Unite 2025
UNITE, powered by the United Negro College Fund (UNCF)
July 20-24, 2025
Atlanta, GA

NACUBO 2025 Annual Meeting
National Association of College and University Business Officers
July 26-29, 2025
National Harbor, MD

NACAC Conference 2025
National Association for College Admission Counseling (NACAC)
September 18-20, 2025
Columbus, OH

URMIA 56th Annual Conference
University Risk Management and Insurance Association
October 12-16, 2025
Las Vegas, NV

2025 Annual Conference
EDUCAUSE
October 27-30, 2025
Nashville, TN

UPCOMING INDUSTRY EVENTS