2024 EDUCAUSE Horizon Report®
Cybersecurity and Privacy Edition

2024 EDUCAUSE Horizon Report®
Cybersecurity and Privacy Edition

THANK YOU TO OUR CYBERSECURITY AND PRIVACY HORIZON REPORT SPONSOR

boldyn NETWORKS

Jenay Robert, Nicole Muscanell, Nichole Arbino, Mark McCormack, and Jamie Reeves,
2024 EDUCAUSE Horizon Report, Cybersecurity and Privacy Edition
(Boulder, CO: EDUCAUSE, 2024).

ISBN: 978-1-933046-21-1

Learn More

Read additional materials on the 2024 Horizon Project research hub,
https://www.educause.edu/horizon-report-cybersecurity-and-privacy-2024

EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision-making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include US and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 100,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information, please visit educause.edu.

CONTENTS

EXECUTIVE SUMMARY

These are, in many ways, tumultuous times. Global political movements and ideologies continue to erode social ties and disrupt state and national legislative processes. Wars in Eastern Europe and the Middle East threaten to destabilize the global order. And new AI-powered technologies are evolving at breakneck speed, offering the world both the promise of new utopian capabilities and the threat of dystopian collapse. Against this backdrop of seismic change, higher education cybersecurity and privacy professionals must navigate new questions around what needs to be done to keep our institutions and our students safe and secure. This report summarizes expert panelist discussions on these and other emerging trends and offers reflections on where the future of higher education may be headed. This project was grounded in a modified Delphi methodology that seeks to elevate the collective perspectives and knowledge of a diverse group of experts, with facilitation tools adapted from the Institute for the Future.

Trends

As a first activity, we asked the Horizon panelists to provide input on the macro trends they believe are going to shape the future of postsecondary cybersecurity and privacy and to provide observable evidence for those trends. To ensure an expansive view of the larger trends serving as context for institutions of higher education, panelists provided input across five trend categories: social, technological, economic, environmental, and political. The panelists selected the following trends as the most important:

Social

- Privacy concerns are growing.
- Cyberattacks that have physical-world consequences are on the rise.
- Cyberattacks targeting students are increasing.

Technological

- Cybersecurity and privacy risks and threats are growing.
- Cyberattacks are increasingly sophisticated.
- Technology is constantly and rapidly changing.

Economic

- Institutions continue to face financial constraints.
- Gaps in the workforce continue to impact institutions.
- AI is increasingly transforming how people work.

Environmental

- Institutions continue to integrate sustainable technologies.
- Pressure is growing for institutions to be sustainable.
- Concerns over the environmental impact of AI are increasing.

Political

- The state and federal regulatory landscapes continue to change.
- Politically motivated attacks are on the rise.
- Politics is influencing higher education programs and curricula.

Key Technologies and Practices

Horizon panelists were asked to describe and vote on the key technologies and practices they believe will have a significant impact on the future of postsecondary cybersecurity and privacy, with a focus on those that are new or for which there appear to be substantial new developments. The following six items rose to the top of a long list of potential technologies and practices:

- AI Governance
- Supporting Agency, Trust, Transparency, and Involvement
- Focusing on Data Security Rather Than the Perimeter
- AI-Enabled Workforce Expansion
- Privacy-Enhancing Technologies
- AI-Supported Cybersecurity Training

Having identified the most important technologies and practices, panelists were then asked to reflect on the impacts those technologies and practices would likely have at an institution. We asked panelists to consider those impacts along several dimensions important to higher education: the importance of those technologies and practices for professionals working in higher education cybersecurity and privacy; the risks that may be introduced or exacerbated by those technologies and practices; and whether and how those technologies and practices might impact diversity, equity, and inclusion.

Scenarios

Scanning the trends and the technologies and practices, we can begin to gather and arrange the information into logical patterns that can help us envision a number of scenarios for the future, scenarios for which we could start to prepare today. In this report, we paint portraits of four possible future scenarios for postsecondary cybersecurity and privacy:

- **Growth:** Forced to choose between better cybersecurity and business as usual, higher education institutions prioritize cybersecurity and privacy funding. There seems to be no limit on what institutions will spend on cybersecurity and privacy, even as budgets for key institutional operations continue to dwindle.
- **Constraint:** Struggling to combat escalating identity theft and fraud, governments work together to implement central identity verification and proofing systems. Independently, stakeholders such as corporations and higher education institutions seek to reduce data footprints by restricting personal device use for employees and students.
- **Collapse:** Political leaders all over the world admit defeat in the global war on cybercrime. Unable to agree on ways to protect citizens and governments, allied nations create border firewalls, segmenting the global internet according to political alliances.
- **Transformation:** Recognizing the growing impacts cybersecurity and privacy breaches have on society, educators integrate cybersecurity and privacy training for learners of all ages. Benefits are far reaching, from educational institutions to the workforce, but some stakeholders are leveraging this important topic as a new way to gain power.

TRENDS: SCANNING THE HORIZON

Since the inaugural information security Horizon Report in 2021, we've seen a number of technological advancements and practices impact not only higher education but society as a whole. Most notably, generative AI is disrupting many institutions globally, causing great concerns over a range of issues including academic dishonesty. Now, conversations about and usage of these newer technologies are expanding. Curiosity and exploration are growing, and institutions are grappling with strategy and policy development so that campus constituents can ethically leverage AI tools and other new technologies to support their work, teaching and learning, and creative endeavors. And not so new to the scene, data continue to be collected on a large scale, now amplified by AI-powered tools. Moving forward, it will be essential for institutions to evolve their cybersecurity and privacy capabilities, paying close attention to the trends and larger forces that shape their technology, data, and infrastructure as they prepare to adapt to changes.

To help us explore these larger forces taking shape around higher education, we asked panelists to survey the landscape and identify the most influential trends shaping cybersecurity and privacy in higher education across five categories: social, technological, economic, environmental, and political (STEEP). This section summarizes the trends the panelists discussed and voted as most important in each of these categories, as well as anticipated impacts of and evidence for each trend.

In this year's report, we see an abundance of evidence pointing to growing cybersecurity and privacy risks and threats for higher education institutions. Cyberattacks targeting students, politically motivated cyberattacks, and cyberattacks with physical-world consequences are all on the rise. These threats will be increasingly difficult to prevent and respond to, given four related trends: technology is constantly and rapidly changing; cyberattacks are becoming more sophisticated (especially due threat actors' use of AI); the state and federal regulatory landscape is changing and is becoming increasingly difficult to navigate; and finally, concerns over the environmental impact of AI are increasing, posing a potential challenge for cybersecurity teams who rely on AI-driven security tools.

New risks are also being introduced as higher education institutions are facing growing pressure to be sustainable and are continuing to integrate sustainable technologies, which tend to expand the cyberattack surface. Institutions are also increasingly implementing AI tools to transform how people work, adding further risks. Unsurprisingly, with the rise in cybersecurity and privacy threats and risks, we also see evidence that privacy concerns are growing—students in particular are becoming increasingly aware of privacy threats and risks and are growing more interested in protecting their data.

Social

Privacy concerns are growing.

Cyberattacks that have physical-world consequences are on the rise.

Cyberattacks targeting students are increasing.

Technological

Cybersecurity and privacy risks and threats are growing.

Cyberattacks are increasingly sophisticated.

Technology is constantly and rapidly changing.

Economic

Institutions continue to face financial constraints.

Gaps in the workforce continue to impact institutions.

AI is increasingly transforming how people work.

Environmental

Institutions continue to integrate sustainable technologies.

Pressure is growing for institutions to be sustainable.

Concerns over the environmental impact of AI are increasing.

Meanwhile, many institutions continue to face financial constraints and workforce gaps, suggesting that colleges and universities need to strategically allocate resources, as well as invest in cybersecurity and privacy training and programs and also in students. These approaches could help support enrollments and retention and develop a pipeline of future cybersecurity and privacy professionals. Moreover, institutions might be in a better position to make these investments, given a promising trend we see this year—politics is influencing higher education programs and curricula. For cybersecurity and privacy, this is a benefit because more government funding is available for higher education cybersecurity and privacy training initiatives.

The summary of these trends is drawn directly from the discussions and inputs provided by our expert panelists, in keeping with the tradition of the Delphi methodology. Each of the trends was identified and voted on by panelists without influence from the EDUCAUSE Horizon Report staff, aside from our work in organizing and synthesizing the panelists' inputs for presentation here.

Each of the trends encompasses far more complexity and variability across types of institutions and regions of the world than can be adequately captured in such a brief summary. Indeed, the expert panelists—who represent a variety of roles and institutional types both within and outside the United States—routinely reflected on the ways in which trends affect institutions differently across different settings. Where possible, we've tried to account for that variability, though the reader will certainly bring additional experiences and contexts that would further broaden these considerations.

Political

The state and federal regulatory landscapes continue to change.

Politically motivated attacks are on the rise.

Politics is influencing higher education programs and curricula.

SOCIAL TRENDS

As the world around us changes and evolves, so too do our needs for more, better, and different approaches to cybersecurity and privacy. Our patterns of human behavior and the social environments in which we find ourselves shape how we interact with the technologies and systems we rely on, and they also shape the ways in which we must protect those technologies, systems, and ourselves.

Privacy concerns are growing.

Impact: Data breaches are continuing to rise globally, and perhaps unsurprisingly so are concerns about privacy. American adults are growing more concerned about their privacy, including how the government and companies are using their data.. This is especially true for young individuals (particularly those in the 18–24 age range). Students are gradually becoming more aware of the vast amounts of data being collected from them, and as a result they might become increasingly proactive in protecting their personal information and data. As student privacy-related views and behaviors evolve, institutions need to be prepared to demonstrate not only their commitment to protecting privacy but also their competency at doing so. As a starting point, institutions should consider growing their privacy capabilities, for example, by establishing a chief privacy officer role and a dedicated privacy office, and by increasing collaborative efforts between cybersecurity and privacy teams. Institutional leaders can also improve or instill trust in students and stakeholders alike by finding ways to introduce and bolster transparency and agency among users to control the collection and use of their data. This can be achieved by developing clearly stated policies and documentation of what data are collected and how they are used, providing notices and obtaining consent/permission, implementing cybersecurity and privacy-by-design methodologies, and providing opt-out methods. Moving forward, institutions will continue to face challenges in protecting privacy. An increasing focus on improving enrollments and the overall student experience will drive the need for enhanced privacy capabilities, as many universities and colleges will not only enhance the services and technologies they offer but will also collect more student data as part of this process, increasing the need for effective data management capabilities (especially data retention policies and practices). Also, a quickly changing compliance and regulatory landscape will require campuses to have adaptable privacy programs/initiatives/policies. And as remote teaching and learning continues, the need for capabilities surrounding broader access to external networks will grow and privacy operations will likely need to be expanded, focusing not only on FERPA and GDPR compliance but also identity and access to protect students and faculty on and off campus. While a rise in privacy concerns presents challenges, it also offers an opportunity for institutions to attract and retain students. By investing in robust privacy capabilities and promoting transparency and autonomy surrounding data and personal rights, universities and colleges might appeal more to students, helping them feel more trust and confidence in their institutions while also experiencing enhanced services that are supported by those robust capabilities.

Evidence: Ohio University is helping students prioritize privacy. The university announced its inaugural student privacy competition, in which students who have taken courses on data cybersecurity and privacy can write an essay on how privacy-related courses they have taken will shape their professional goals and responsibilities. The University of Michigan is making its data collection practices more transparent. The institution offers a website called ViziBLUE, which shows what types of personal information are collected and how that information is used and shared.

Cyberattacks that have physical-world consequences are on the rise.

Impact: Concerns about cyber-physical attacks are growing, especially those generated via AI. Although cyber-physical attacks directly target physical systems and infrastructure, physical consequences such as operational disruptions can also stem indirectly from breaches. For example, the University of Michigan shut down internet connections in response to a cybersecurity concern, disrupting campus IT systems and a number of business functions across the institution for two days. In extreme cases, cyberattacks can even cause physical harm and death. As cyberattacks with physical consequences increase, institutions and their critical infrastructure and operations will be subject to a greater number and variety of attacks, especially those supporting federal government projects, medical/health communities, and industrial systems/operations. With the proliferation of analytics, the Internet of Things (IoT), and the convergence of IT and operational technology (OT), institutions are increasingly relying on internet-enabled devices to control OT functions including power, HVAC, water, machinery, vehicles, and supply chain processes. As threats evolve, institutions could see a rise in ransomware aiming to take these functions/systems (instead of data) hostage, directly impacting business operations and daily living. To combat these threats, greater burden will be placed on IT, cybersecurity, and facilities operations departments, increasing the scope of what needs to be protected. Leaders and staff from these departments will increasingly need to collaborate

and engage in awareness and threat analysis, in addition to preparing business continuity and disaster plans at a greater scale. Universities and colleges might also need to reconsider crisis teams and management plans to include cyber-incident response, in addition to investing in employee up- and re-skilling, given that proper management and responses may require new skills and expertise for existing cybersecurity, privacy, and IT professionals. Institutions might also need to revise their cybersecurity operations center frameworks to account for cybersecurity of critical infrastructures and systems.

Evidence: According to a recent threat report by Waterfall cybersecurity, "at least 68 cyberattacks last year caused physical consequences to OT networks at more than 500 sites worldwide." This number increased by almost 20% from 2022. The government now considers higher education institutions to be as critical infrastructure, and they might be required to report incidents under the proposed Cyber Incidents Reporting For Critical Infrastructure Act (CIRCIA).

Cyberattacks targeting students are increasing.

Impact: The education sector is increasingly being impacted by data breaches. Not only is student data as a whole being targeted more frequently via attacks on directories, databases, and other information storage systems, but students are being directly targeted via phishing and ransomware attacks and are increasingly falling victim to such attacks. This growth in vulnerability of young people is notable given that older adults are often thought of as being most vulnerable to cyberthreats and attacks. Yet, recent findings suggest that this is changing: Gen-Z is more prone to being attacked than Boomers. Over the years (and recently) students have been targeted by numerous cyber scams disguised as student loan relief, scholarship and grant opportunities, job offers, online program recruitment, and listings for apartments, books, and moving services. Threat actors have also taken aim at social media users, with some students recently being victims of violent, graphic, and sexually-based (e.g., "sextortion") ransomware attacks. One factor driving the rise in attacks on students is their financial instability. Many students are struggling with rising tuition, inflation, and cost of living, not to mention not having yet entered a stable career. This leaves them more vulnerable to threats promising quick financial benefits. The impacts of cyberattacks on students and their data extend beyond just direct financial loss and legal repercussions for institutions. Affected students may not be able to continue with their studies if they incur monetary setbacks from scams, and student trust in their institutions and leadership could be diminished if breaches and other incidents occur. Both could further compound ongoing enrollment and retention issues. The psychological impacts of cyber-victimization such as stress, anxiety, and feelings of loss of control that are typically associated with being a victim of a cyberattack could also diminish the student experience, placing turmoil on students, many of whom already struggle with mental health and well-being challenges. Finally, recent reports show that threat actors are increasingly targeting ethnic minorities and international students. Unchecked, this could further widen existing systemic gaps in education. With growing threats to students, institutions should find ways to empower students to be active players in protecting their privacy and the campus as a whole. Institutions should invest in robust and engaging (and ongoing) cybersecurity and privacy awareness training programs that are student-centric, in addition to widely incorporating these topics into degree programs (not just for those enrolled in computer science, IT, and cybersecurity-related fields). Training and curriculum should not only focus on students' use of technology on campus but also include off-campus use, including personal devices and platforms such as social media. Finally, as phishing emails are increasingly being used to target students, one step that institutions can take is to improve their email security so that compromised accounts are not used to defraud students.

Evidence: According to the Federal Trade Commission, job interview scams targeting students are getting increasingly personal. Threat actors are increasingly approaching students via personalized social media and email messages, claiming, for example, to have a connection to a specific college or university and its leaders. The University of Denver's IT and marketing departments worked together to engage students in cybersecurity awareness. As part of these efforts, the university dressed up dogs as fish, grabbing interest from students. Students who stopped to visit the dogs learned about phishing and were given opportunities to win incentives.

FURTHER READING

Center for Strategic & International Studies
"The Right to Be Left Alone: Privacy in a Rapidly Changing World"

U.S. Department of Homeland Security
"Cyber Physical Systems Security"

WIRED
"The Hidden Injustice of Cyberattacks"

TECHNOLOGICAL TRENDS

The types of technologies we use, the connections we build between those technologies and larger information systems and networks, and the ways in which we integrate all of this into our personal and professional lives—these ingredients constitute the technological ecosystem within which we live. Whether that technological ecosystem remains safe and protected depends on the ability of cybersecurity and privacy professionals and practices to keep pace with that ecosystem's ever-changing features and boundaries.

Cybersecurity and privacy risks and threats are growing.

Impact: The cybersecurity and privacy threats and risks that higher education institutions face are growing. Many saw an increase in ransomware, malware, and phishing attacks, as well as compromises/breaches related to third-party services, and now compromises related to the use of AI tools such as ChatGPT are being added to the mix. The education sector is an increasingly attractive target for threat actors because educational institutions contain lots of stored sensitive data, they have complex IT environments (e.g., legacy systems and decentralized infrastructures), user compliance is challenging, and their cybersecurity and privacy teams are increasingly working under constrained conditions. Adding to this, threats and risks are growing due to changes in culture, technology, and policy and regulations. For example, the move to remote teaching and learning, the rise of AI and immersive technologies, a focus on student success and personalized learning, and IoT integration—just to name a few—have all added new cybersecurity and privacy challenges and risks. Because cyberthreats and associated risks are unlikely to subside, the most obvious step is for universities and colleges to increase and mature their cybersecurity efforts—implementing appropriate cybersecurity frameworks; conducting risk assessments and cybersecurity audits; implementing robust and, in some cases, tighter controls and guardrails; investing in awareness and training; and implementing policies/procedures that ensure compliance and that provide clear guidance to stakeholders surrounding their data and use of devices. Yet to keep up and make necessary improvements in each of these areas, institutions will need to overcome the challenge of limited resources. Recent work shows that cybersecurity and privacy professionals are operating in reactive mode, focusing much more on incident response as opposed to preventative strategies due to workforce gaps and staffing and workload issues. This is impeding their ability to execute balanced cybersecurity and privacy operations, and it leaves important areas of cybersecurity neglected (e.g., preventative approaches such as monitoring and scanning for early detection). Institutions must find ways to support balanced and comprehensive cybersecurity and privacy efforts. By ensuring that professionals have enough time to devote to minimizing risks in addition to having strong response capabilities, institutions can save more money.

Evidence: According to an article in *Nature*, cyberattacks on knowledge institutions are increasing, and some of the biggest cybersecurity risks stem from the use of weak passwords and systems that are accessed via MFA. Further, experts are predicting that the recent massive MOVEit attack is going to spawn similar attacks against higher education, with some experts noting that MOVEit is "serving as a green light" for other attacks, given its success. The Readiness and Emergency Management for Schools (REMS) offers resources for cybersecurity preparedness for K–12 and higher education institutions.

Cyberattacks are increasingly sophisticated.

Impact: Cyberattacks are becoming more sophisticated, and this will likely continue as technology advances and threat actors look for workarounds to existing and newer forms of cybersecurity measures. Unsurprisingly, AI is playing a significant role, making cyberattacks more efficient, adaptable, believable, and precise. AI can be used by threat actors to automate profiling and reconnaissance, personalize attacks (e.g., tailoring attacks to specific individuals, deepfakes), and create increasingly intelligent and responsive attacks as machine learning algorithms are capable of learning and adapting in real time. In addition to incorporating AI, threat actors are changing their tactics, finding ways to compromise MFA and utilizing encryption-free extortion and double extortion tactics. As cyberattacks become more sophisticated, institutions will face the challenge of not only keeping up but also staying ahead of emerging threats. Traditional protection strategies and systems may be rendered ineffective and as such will need to be continuously assessed; newer protection capabilities may need to be implemented. Institutions might need to consider utilizing a mesh approach—integrating various cybersecurity threat monitoring, detection, alerting, and prevention capabilities to work together to form more actionable intelligence and proactive threat management. Cybersecurity and risk management leaders will need to invest in identity and access management solutions to help

mitigate the risks of AI-driven attacks, for example by adopting technology that can prove genuine human presence. More stringent controls and verification processes will need to be implemented, and institutions will need to double-down on awareness training. Fostering a culture of continuous learning and adaptability and involving all stakeholders will be key. As communication surrounding cyberattacks increases (within and across institutions), the evolution of cyberattacks and threat actor tactics will become more visible and identifiable. Finally, institutions may need to resort to "fighting fire with fire"—that is, while AI poses threats, it also presents opportunities to harness its powers to combat and prevent cyberattacks. AI will be able to detect cyberthreats beyond social and audio/visual threats via capabilities such as predictive pattern analysis of networks and highly automated and rapid adjustment to remediation. Integrating AI technologies into cybersecurity systems could help institutions refine their monitoring and detection capabilities, allowing them to more precisely and quickly detect anomalies. Institutions should also consider partnering with vendors that are leveraging AI for cybersecurity (with caution, of course).

Evidence: According to a recent article, AI is being leveraged to create advanced social engineering attacks by aiding in the creation of sophisticated emails, creating deepfakes, cloning human speech and audio (e.g., for voice phishing), and automating steps, helping deploy large-scale attacks. The University of California, Santa Barbara received $20 million from the NSF for its Agent-based Cyber Threat Intelligence and Operation (ACTION) Institute, which aims to develop next-level AI-powered cybersecurity operations.

Technology is constantly and rapidly changing.

Impact: According to a recent report, "the pace of technological change is much faster now than it has been in the past." For example, "it took 2.4 million years for our ancestors to control fire and use it for cooking, but 66 years to go from first flight to humans landing on the moon." AI is a big driver in the speed of change. As AI advances, we might see technology change at an even faster rate. This presents an obvious challenge for cybersecurity and privacy teams. AI is developing so fast that we can't keep up—especially, but not only, on the regulation side. Some speculate that a new generation of computing (quantum computing) is going to arrive sooner than expected and, combined with AI, has the potential to "be millions of times faster than the fastest microchip computers today." Currently, the regulatory landscape excludes AI-related risks, but that will undoubtedly change in the near future. Institutions need to be prepared to update their cybersecurity strategies and policies once AI is added to the regulation/compliance mix. The speed of change is and will continue to be a challenge for higher education institutions in particular because traditionally the sector has been slow to change. Institutions will need to find ways to keep pace (or ideally, ahead of developments), without rushing processes, which can lead to mistakes and could make cybersecurity efforts less effective. Similar to the trends of an increase in cyberattacks, some methods may already be (or will soon become) outdated and ineffective. Traditional cybersecurity approaches rely on known threat signals and can often be rules-based and reactionary. Institutional leaders who haven't done so will need to consider newer adaptive approaches to cybersecurity. These approaches should lean on continuous monitoring and real-time adaptations and should have a balanced focus on both prevention and response. As part of this, not only should strategic approaches be up to date, but so should the technology and infrastructure. While awareness and training for users is a solution for a number of trends (including ones already discussed), equally important is the investment in training for cybersecurity, privacy, and technology leaders and professionals at higher education institutions. With accelerated advancements in technology will come new risks. Professionals and leaders will undoubtedly need to continuously learn new skills, technologies, legal information, and frameworks to ensure their initiatives remain sustainable. Institutions will need to put more resources into providing these individuals with up- and re-skilling opportunities on a regular basis, in addition to ensuring that they have time to participate in such training.

Evidence: According to a report by Infosys, "nearly three-quarters (71%) of respondents admitted to worrying that the pace of technology change exceeds their organization's ability to learn how to incorporate it into operations." Our World in Data maintains a web page devoted to the significant technological changes shaping societies. The page offers data, visualizations, and articles on a gamut of topics including changes in computers, the internet, AI, social media, and communication technologies.

FURTHER READING

Verizon Business
"2024 Data Breach Investigations Report"

Fortune
"Countering AI-Driven Cyberattacks with AI-Driven Cybersecurity"

McKinsey & Company
"As Gen AI Advances, Regulators—and Risk Functions—Rush to Keep Pace"

ECONOMIC TRENDS

Higher education faces enrollment and revenue challenges on the road ahead, and many institutions might need to rethink their business models, reduce their size and spending, join or collaborate with other institutions, or shutter their doors. Any combination of these adjustments in the future will make new demands of, and have lasting implications for, cybersecurity and privacy in higher education.

Institutions continue to face financial constraints.

Impact: With declining enrollments and rising costs, institutions continue to face financial constraints, necessitating budget cuts across departments and areas. Although 2023–24 federal funding will largely remain the same for higher education, many institutions will still have to continue with the "do more with less" approach. Interestingly, cybersecurity departments and units have seen recent increases in budgets. However, these increases are essentially only allowing many cybersecurity and privacy teams to keep up with inflation. Further, increased funding for cybersecurity and privacy often comes at the expense of IT operations since these areas tend to share a budget, ultimately lowering its security posture by opening the door to additional IT-related threats. With continuing financial constraints, universities and colleges will need to allocate resources strategically, prioritizing areas of expenditure based on criticality. One step that institutions can take to minimize costs is to leverage risk frameworks to guide efforts and inform spending. Conducting a risk assessment can help institutions identify the most critical assets, allowing cybersecurity and privacy teams to use their limited resources to protect these. Institutions should also conduct inventories of their current cybersecurity infrastructure and tools, looking specifically for ways to consolidate functionalities and eliminate redundant tools/processes and unused/unneeded resources. The same goes for services—a careful analysis of services can help teams identify costs and determine whether offering specific services in-house versus outsourcing them makes the most sense financially and operationally. Institutions can also leverage AI to help automate certain processes, though they should be cautious as they do so. Maintaining productivity with fewer and fewer resources may tempt some to adopt AI tools that have not been rigorously tested, which could increase cybersecurity and privacy risks. Finally, while it is important for universities and colleges to have comprehensive and balanced cybersecurity and privacy programs, they should also look specifically to enhance their response and recovery efforts. Doing so will ensure they are able to manage incidents in a consistent and programmatic way so that in the event of a major incident, attention is not diverted from proactive cybersecurity and privacy programs, helping minimize associated financial losses.

Evidence: A recent report found that the biggest obstacle for strategic cybersecurity execution in 2023 was limited budgets, which jumped ahead of other challenges including skills gaps, executive-level buy-in, and making sound technology investment decisions. An article in *Harvard Business Review* outlines cybersecurity strategies for organizations with limited cybersecurity budgets. The article discusses cybersecurity investments in three main areas: defense controls, measures-validating controls, and automation.

Gaps in the workforce continue to impact institutions.

Impact: Cybersecurity and privacy workforce gaps continue to be a challenge for many industries, and higher education is no exception. According to a recent article, "The global cybersecurity workforce gap has reached four million people, a 12.6% increase compared to 2022." Further, skills gaps are posing just as many challenges as workforce shortages. A study by ISC2 found that almost 60% of cybersecurity workers said that skills gaps are more challenging than staff shortages. The privacy workforce faces similar challenges, some of which are likely compounded by the fact that privacy is a younger discipline. In higher education, workforce challenges are particularly difficult to resolve given increasing financial constraints and compensation that is far less competitive than industry (though according to the ISC2 report, some of the recent workforce shortages are being caused by layoffs, and as a result higher education might find itself in a better position to recruit talent.) As threats grow, the need for cybersecurity and privacy professionals will also grow, putting higher education in a position to help address these gaps by investing in the development of both traditional and nontraditional training and programs focused on cybersecurity and privacy training. Some institutions have already begun this journey, developing colleges and academic programs in addition to offering students opportunities to gain hands-on experience. By investing in students, institutions can develop a workforce pipeline, training young people who can then enter the workforce and fill those gaps. Institutions will need to also invest in their existing workforce—recent research shows that staffing issues combined with ongoing budget constraints are increasing workloads, leaving some areas of cybersecurity and privacy neglected. Moving forward, institutions need to

find ways to support the professional development of their current staff. By offering regular opportunities to up- and re-skill, institutions can help decrease the skills gap and retain talent. Finally, institutions will need to continue with their efforts in improving enrollments and retention. With, among other challenges, the looming enrollment cliff and declining views of the value of higher education, all degree programs could potentially suffer, including those needed for training new generations of cybersecurity and privacy professionals. Institutions may want to consider forming early partnerships with K–12, working together to bring awareness to cybersecurity and privacy and garnering interest in students well before they consider entering college.

Evidence: Google is partnering with the Consortium of Cybersecurity Clinics to provide support to universities and colleges in an effort to increase access and opportunities for students pursuing careers in cybersecurity. LSU Shreveport is hiring student workers at their cybersecurity Operations center in an effort to give students a chance to develop skills while also addressing gaps in the cybersecurity workforce. Hired students gain hands-on experience in handling cybersecurity alerts, analyzing malware, and learning about attacker trends.

AI is increasingly transforming how people work.

Impact: Discussions surrounding AI's potential impacts on the economy and workforce are ongoing, leaving many worried that it will replace their jobs. More likely, AI will have both positive and negative impacts on the workforce, replacing some jobs, yes, but also helping improve or create others. Higher education has already begun investing in AI-powered tools to address a number of challenges, including supporting student success, streamlining administrative tasks, and improving operational efficiency. Given the financial constraints and uncertainty in the future of enrollments, AI seems to be a viable and practical solution for maintaining operations with limited people and resources. Yet as institutions continue to explore and implement AI solutions to meet their needs, this will introduce new cybersecurity and privacy risks and challenges. A recent opinion piece suggests that as institutions continue to explore AI workflow solutions, the following areas could be impacted: marketing and campus relations, admissions and enrollment, finance and administration, libraries, faculty, and student services (advising, tutoring). Implementation of AI more broadly across these areas of the institution will increase attack entry points, in addition to the amount of data being collected and thus needing protection. For cybersecurity and privacy professionals, AI will most likely make their work both more and less challenging. It will aid in cybersecurity efforts, helping automate processes; speed up hunting, detection, and response efforts; and increase precision. Yet it will also introduce new risks across the institution, placing more burden on cybersecurity and privacy teams (who are already working in constrained conditions). To support cybersecurity and privacy professionals, institutions will need to invest in professional development and training specific to AI, ensuring that these individuals have the knowledge and skills to manage and protect such tools. Additionally, institutions will need to ensure that there is an effective process for evaluating and implementing these tools, being careful not to rush into adoption and only doing so after thoroughly evaluating the potential risks and whether they outweigh the benefits.

Evidence: Microsoft released a report that examines how AI will reshape work and the labor market across 31 countries. The findings show that although employees want AI at work, many fear job loss due to AI. Amid growing concerns about job loss, federal IT leaders addressed these fears, stating that "automation will not replace humans." Leaders noted that there is no shortage of work in the cybersecurity industry and that cybersecurity professionals should expect AI to be more like a personal assistant, helping increase productivity.

FURTHER READING

Higher Ed Dive
"Inflation Will Continue to Batter Colleges through Fiscal 2024, Moody's Predicts"

World Economic Forum
"The Cybersecurity Industry Has an Urgent Talent Shortage. Here's How to Plug the Gap"

McKinsey Global Institute
"Generative AI: How Will It Affect Future Jobs and Workflows?"

ENVIRONMENTAL TRENDS

Our depletion and pollution of the natural world is contributing to a worsening of and more extreme environmental conditions. While technological innovations are helping us better understand and even curb these environmental trends, those innovations also transform our information and technological landscape in ways that necessitate new strategies for cybersecurity and privacy.

Institutions continue to integrate sustainable technologies.

Impact: As climate change continues to impact the environment and people globally, universities and colleges are continuing to invest in sustainability. As part of this, some institutions have integrated energy-saving technologies to reduce their carbon footprints, including solar-powered technologies; energy-efficient/optimizing lighting, heating, and cooling systems; and waste/recycling technologies. Moreover, institutions are increasingly looking to build smart buildings and campuses powered by AI technologies as a means of conserving energy. The continued integration of such technologies is raising concerns about associated cyber risks and threats. A recent study found that a majority of cybersecurity decision-makers are "concerned that these new technology deployments—which could span cloud computing, renewable energy infrastructure and smart grids—will expand the cyberattack surface and number of entry points across [critical national infrastructure] networks." Institutions looking to adopt sustainable technologies should consider using a secure-by-design approach, adopting sustainable technologies that are designed from the outset with integrated cybersecurity measures. As part of this, there should also be careful review and consideration of third-party providers' data management and protection practices and whether adoption would impact compliance with regulatory requirements. One challenge institutions will face is in taking the appropriate amount of time to review and understand new and emerging technologies in a landscape where technology is changing so rapidly and pressure to adopt new solutions is growing. They will need to find ways to adopt sustainable technologies in a timeframe that is timely, yet not too rapid, allowing them to keep up with innovation and knowledge advancement while reducing emissions. To ensure that the adoption and implementation of such technologies is effective and successful, cybersecurity and privacy teams will need access to training and development opportunities so that they can understand and identify emerging threats, in addition to acquiring skills required to safely integrate these tools into existing systems.

Evidence: Universities and colleges are increasingly adopting sustainable technologies at their campuses by taking advantage of the Biden-Harris Administration's Inflation Reduction Act (IRA). The IRA provides higher education institutions with opportunities to use tax credits and deductions to support their investment in clean energy. According to findings from a report on cybersecurity leaders, more than 80% of organizations in the United States believe that environmental challenges are hindering their cybersecurity efforts. The report also found 84% of U.S. critical infrastructure to be "at heightened risk by the effects of climate change, with new sustainable technologies exposing organizations to greater cybersecurity threats."

Pressure is growing for institutions to be sustainable.

Impact: Higher education institutions are facing increasing pressure to be climate friendly, and a lot of this pressure is coming from students. Recent findings showed that 87% of students believe that their college or university should take sustainability seriously, and internationally, a growing number of students are demanding that their institutions divest from companies with fossil-fuel ties. As universities and colleges increase their commitment to sustainability, they will not only adopt new and emerging technologies but also make changes to their physical infrastructure, such as by relying more on IoT integration and AI-powered systems, which will increase their vulnerability to a variety of cyberthreats. Institutions are also increasingly integrating environmental, social, and governance (ESG) principles into their decision-making processes, yet it is unclear to what extent cybersecurity and privacy goals are part of this. Gartner predicts that "30% of large organizations will have publicly shared ESG goals focused on cybersecurity by 2026." Moving forward, institutions need to recognize the importance of aligning their cybersecurity and privacy and ESG efforts to achieve long-term sustainability and resilience. By integrating cybersecurity and privacy considerations into their broader ESG frameworks, universities and colleges can proactively address emerging risks, mitigate reputational

damage, and uphold their commitments to sustainability and responsible governance. To achieve this, collaboration needs to happen across departments and stakeholders so that cybersecurity, privacy, and ESG considerations are integrated seamlessly into governance structures, risk management frameworks, and strategic decision-making processes. Finally, in some cases, the goal of being sustainable may compete with cybersecurity and privacy goals. That is, for cybersecurity and privacy teams to protect individuals and data, they may need to rely increasingly on energy-consuming technologies and methods, counteracting sustainability efforts. To combat this, institutions can look for ways to reduce their cybersecurity and privacy emissions, for example by using cloud-based solutions, outsourcing services from eco-friendly vendors, rethinking data storage solutions and practices, and investing in green devices (e.g., built from recycled materials). Institutions can also reduce the amount of e-waste they produce by adopting technologies and services that have sufficient security support for devices, especially as they age. Finally, institutions can also invest in robust privacy programs that focus strongly on data governance and management practices that reduce data collection and retention, thereby reducing computing and storage emissions.

Evidence: With growing pressures to be sustainable, higher education institutions should consider the cyber resilience of sustainable infrastructures and technologies on their campuses. An article from *WIRED* discusses renewable technologies and the importance of making these technologies cyber resilient. Institutions should develop an understanding of the relationship between cybersecurity, privacy, and sustainability and the role their cybersecurity and privacy professionals play in supporting sustainability.

Concerns over the environmental impact of AI are increasing.

Impact: Concerns about AI's impact on the environment are growing. These concerns include the use of nonrenewable materials to create hardware supporting AI and the consumption of energy and natural resources that is involved with AI computing and data storage. This poses a problem for cybersecurity and privacy teams in higher education, given that AI is an increasingly viable option for detecting threats and protecting data. As institutions look to improve their sustainability efforts, they will need to consider their use of AI carefully. Teams relying on AI-driven cybersecurity measures will not only need to be mindful of the carbon emissions produced by them but will also need to find ways to reduce these emissions. As a first step, institutions should consider monitoring and tracking their AI-related emissions, which will provide an understanding of how much they will need to reduce their emissions. Second, cybersecurity and privacy teams can look for ways to make their AI consumption more environmentally friendly, for example by investing in AI-powered cybersecurity solutions that either don't require large language models (LLMs) at all or rely on existing ones (rather than creating new ones), incorporating fine-tuning methods (improving model efficiency), and using low-powered devices to run models. Institutional leaders could also consider adopting cybersecurity solutions that use specialized small lightweight models (SLMs), which are a more streamlined version of LLMs, requiring less data and resources for training. Because they are smaller and streamlined, they are able to make computations much more quickly and ultimately have a significantly smaller carbon footprint compared to LLMs. SLMs can potentially revolutionize cybersecurity and privacy by enhancing threat detection and risk assessment with unprecedented efficiency, affordability, and accuracy, while improving energy efficiency. However, these models are just beginning to gain popularity, and thus, SLM-driven cybersecurity solutions may not be widely available. In the meantime, universities and colleges may need to limit their use of AI-driven cybersecurity tools or find ways to reduce emissions in other areas of operation to counteract the impact of these tools.

Evidence: Researchers at Hugging Face and Carnegie Mellon University recently carried out the first attempt at estimating the carbon footprint of a large language model. The Green Algorithms project offers resources promoting environmentally sustainable computational science practices. It provides calculators that researchers can use to estimate the carbon footprint of their projects, tips on how to be more environmentally friendly, training material, past talks, and other resources. A recent article in *Nature* found that AI can carry out some tasks such as writing and illustration at much lower carbon emission levels than humans.

FURTHER READING

Reuters
"SEC Cybersecurity and Climate Rules: Where Are They Now?"

Cybersecurity & Infrastructure Security Agency
"Extreme Weather and Climate Change"

Scientific American
"AI's Climate Impact Goes beyond Its Emissions"

POLITICAL TRENDS

Higher education, for better and for worse, is always entangled in and concerned with the political climate and events of the present moment. In addition to determining overall higher education funding, politics is interwoven with higher education as an object of research and study and as subject matter for courses. Because of this long-standing entanglement, political trends have significant effects—both positive and negative—on cybersecurity and privacy in higher education at a variety of levels.

The state and federal regulatory landscapes continue to change.

Impact: Navigating the changing state and federal regulatory landscape continues to be a challenge for most higher education institutions. Recently a number of federal-level changes have been either proposed or enacted. The Federal Acquisition Regulation (FAR) Council set forth two proposals: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems and Cyber Threat and Incident Reporting and Information Sharing. These proposed rules would increase requirements for contractors and would expand the scope and reach of federal agencies. Changes were made to FERPA (new guidance issued on student health records); the NIST SP 800-171 and the CMMC model and certification process were revised with new rules for protecting controlled unclassified information (CUI); and the Gramm-Leach-Bliley (GLBA) Safeguards Rule was updated (increasing incident reporting requirements). And, more recently, the U.S. Department of Homeland Security (DHS) Cybersecurity Infrastructure and Security Agency (CISA) published a proposal to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). According to this act, many higher education institutions might qualify as "covered entities" and would be subject to additional incident reporting requirements such as the reporting of covered incidents, ransom payments made, and new or different information discovered related to a previously submitted report. Local and state regulations add to the complexity of regulations and compliance. There is variability in legislative pursuits when it comes to cybersecurity and privacy-related issues. For example, some states (but not all) are passing their own Biometric Information Privacy Acts (BIPAs) in an attempt to better protect consumer health data. Yet a recent report suggests that state privacy legislation has not reached a high level of efficacy, especially due to a lack of federal privacy laws. This has led to variability in definitions surrounding privacy matters, making some legislation more effective and some less effective. Finally, the lack of regulations surrounding AI is on the minds of most, and with an increasing focus on strengthening privacy protections, enforcing privacy laws, and establishing AI regulations (nationally and internationally), even more changes are on the horizon. What does all of this mean for cybersecurity and privacy professionals in higher education? For the most part, it means increased burden. Cybersecurity and privacy professionals may find it increasingly challenging to navigate the regulatory landscape, and cybersecurity and privacy departments/units will be faced with larger workloads and increased costs as regulatory changes necessitate revisions/upgrades to cybersecurity and privacy programs, systems, and processes to maintain compliance and meet CMMC certification requirements. Some of these changes could also increase risks associated with enforcement (i.e., for institutions that experience a cybersecurity incident requiring notification to the Federal Trade Commission). Ultimately, this will increase the need for universities and colleges to establish privacy programs and roles and communities of practice related to common privacy principles such as trust, transparency, and consent. Privacy professionals are often the primary stakeholders on campus who understand the intricacies of the complex web of state, federal, and international laws that affect personal information. Placing privacy responsibilities on the shoulders of non-privacy professionals will be cumbersome and would require extensive training so that sound decisions could be made from a legal perspective. Moving forward, institutions can take a number of steps to facilitate their compliance, including conducting regular data audits, implementing privacy-by-design initiatives, establishing transparent policies along with a clear process for informed consent, appointing data protection officers, and investing in training and legal advice (especially for those who are not able to establish stand-alone privacy roles). And of course, institutions will need strong collaboration between cybersecurity, privacy, legal/compliance, and technology teams to meet the plethora of existing and upcoming changes in regulations.

Evidence: The IAPP Westin Research Center tracks proposed and enacted comprehensive privacy bills across the United States. The tracker can help institutions understand how privacy is developing from a regulatory perspective. Recently, EDUCAUSE responded to research cybersecurity regulations in Q1 2024 and the proposed net neutrality rule.

Politically motivated attacks are on the rise.

Impact: A number of countries have lately experienced an increase in politically motivated attacks, especially distributed-denial-of-service (DDoS) attacks. A recent report suggests that DDoS attacks increased by 15%, with many politically motivated. Hacktivist groups have also recently targeted higher education institutions. Hacktivist groups are thought to be responsible for recent attacks on UK universities, Israeli universities, and the University of Michigan Health. It should be noted that thus far, the uptick in politically motivated cyberattacks seems to be linked to a handful of threat actors and is not a result of a spike in the number of threat actors. Although cyberattacks on higher education institutions continue to rise, it's unclear what portion of these are politically motivated. Yet, with a contentious U.S. presidential election looming, in addition to ongoing political tensions on campuses and debates about higher education and its values, politically motivated attacks on universities and colleges could increase. So what can cybersecurity and privacy teams do to mitigate these risks, aside from enhancing their cybersecurity measures? Institutions may need to implement additional safeguards for work tied to the federal government, as federal projects may be more vulnerable to politically motivated attacks. Cybersecurity and privacy professionals may also look to collaborate with professionals who have expertise in politics and international relations (within and across institutions). Through such collaborations, new methods for identifying key risks to the institution based on politically motivated attacks could be developed. Institutions can also utilize publicly available information to monitor the activity of known hacktivists and nation-state cyber actors. For example, Microsoft recently profiled known nation-state threat actors that are using LLMs to enhance their attacks. Universities and colleges should also strengthen their physical infrastructures as a means of mitigating political threats. Last year, the Biden administration announced an action plan to combat antisemitism on higher education campuses, and as part of this, advisers from CISA are advising institutions on how to make their campuses safer from physical threats and attacks.

Evidence: The Digital and Cyberspace Policy program offers a Cyber Operations Tracker, which is a database of publicly known state-sponsored incidents that have occurred since 2005. The tracker can be searched by incident type, threat actor, and keywords. The Center for Strategic & International Studies provides a timeline of significant cyber incidents since 2006, focusing specifically on cyberattacks targeting government agencies, defense and high-tech companies, and economic crimes with losses greater than $1 million.

Politics is influencing higher education programs and curricula.

Impact: Government influence on academic programs and curricula continues to be a contentious subject; especially of concern is the issue of academic freedom. Yet in the midst of these growing concerns, prospects are not all doom and gloom for cybersecurity and privacy. In fact, more government support—from both the federal and state governments—will be available soon to expand cybersecurity training initiatives in higher education. For example, the Department of State allocated $100 million for CHIPS and Science Act projects, which includes funding for partnerships between industry, universities, and research institutions that will work together to enable environments for secure information and communications technology (ICT) ecosystems. More recently, the Biden-Harris Administration announced a National Cyber Workforce and Education Strategy that fully considers investment in cybersecurity training across sections, including higher education. The strategy seeks to build and enhance collaboration around four pillars: (1) equip every American with foundational cyber skills; (2) transform cyber education; (3) expand and enhance the national cyber workforce; and (4) strengthen the federal cyber workforce. The Biden-Harris Administration is also increasing its efforts toward protecting privacy. Recently, the administration issued an executive order to protect Americans' sensitive personal data. State and local governments are also increasing their support for cybersecurity and privacy in higher education, providing increased funding for the development of new training programs and centers,

as well as collaborations and partnerships. With these growing efforts and investments from the government, higher education institutions will increasingly be in a position to develop and/or expand cybersecurity and privacy curricula to help fulfill new government strategies and initiatives. This could help institutions attract new students, thus alleviating ongoing financial concerns in addition to addressing gaps in the cybersecurity and privacy workforce. As institutions expand their cybersecurity and privacy training options, they may also have access to more in-house professional development and awareness and training opportunities for staff, allowing them to keep cybersecurity and privacy capabilities up to date, thus mitigating cyberthreats and risks.

Evidence: Fresno State is partnering with California State University, San Bernardino, and San Jose State to offer a pilot program focused on developing innovative collaboration with key stakeholders and partners to promote career pathways for cybersecurity and emerging technology industries. According to a recent newsletter, "The partnership, named Workforce Innovation Technology Hub, or WITH-Cyber, is funded by $4 million from the state's cybersecurity Regional Alliances and Multistakeholder Partnership Pilot Program." The White House recently released the federal FY25 budget, which calls for $13 billion in cybersecurity funding for civilian agencies.

FURTHER READING

The Consortium for School Networking
"Summary of Education Cybersecurity Policy Developments in 2023"

Center for Strategic & International Studies
"AI Regulation is Coming—What Is the Likely Outcome?"

World Economic Forum
"Global Cybersecurity Outlook 2024"

KEY TECHNOLOGIES & PRACTICES

The Horizon Report describes "key technologies and practices" that are anticipated to have a significant impact on the future of cybersecurity and privacy in light of the social, technological, environmental, economic, and political trends previously identified by the panel. In the nomination and voting process, panelists consider which technologies or practices have the most potential to either mitigate or accelerate these trends. We include technologies and practices because we know that while innovations and advancements in technological capability create new opportunities, it's often the daily cybersecurity and privacy practices or the development of institutional capabilities that offer the most potential as change drivers. In this section, readers will find an overview of each key technology or practice, ideas for action, and a set of resources for further reading. Brief descriptions of examples of projects that bring the technologies and practices to life are also included.

AI GOVERNANCE

Overview

As more institutions adopt AI-powered tools for learning and work, AI governance will be vital for protecting institutions and individuals. Unless AI governance is in place before new tools are adopted, institutions risk exposing themselves to cybersecurity threats, infringing on end users' privacy, reinforcing systemic inequities, and violating the complex web of data-related regulations. Companies that are rapidly expanding their use of AI might be prioritizing speed over cybersecurity and privacy, and institutional leaders cannot safely assume that every new AI tool and feature will adequately safeguard users and institutional data. Still, cybersecurity and privacy professionals must balance this need to be cautious against the desire for rapid adoption of AI tools in higher education. AI governance that is too restrictive or rigid might generate resentment, stifle innovation, and even simply be ignored by stakeholders who are eager to adopt new tools.

> ***"Establishing a framework for decision-making around AI adoption will help ensure that AI is used responsibly, with full consideration of potential impacts on the security and privacy of our institutional data."***

Certainly, creating and maintaining effective AI governance is much easier said than done. Institutions face myriad challenges in any data governance endeavor, but AI presents a uniquely complex challenge. First, the technology itself can be difficult for professionals outside the field to understand how it works, and "how it works" is a moving target. For these reasons, threats to cybersecurity and privacy can be equally opaque and dynamic. Second, AI tools frequently leverage a variety of data processes and systems. Even when individual data governance elements work well to protect cybersecurity and privacy, a combination of elements might lend itself to exposure, exploitability, and impact. Finally, AI technology is now being integrated into most software, even that which is not primarily powered by AI. Such ubiquity makes it difficult for cybersecurity and privacy professionals to understand the actual attack surface and supply chain. These challenges underscore the importance of taking a collaborative approach to AI governance, including colleagues from across the institution in decision-making and ongoing processes.

> ***"AI systems and the infrastructure and processes that create them still have poorly understood elements that cloud visibility to all their potential attack surfaces and vulnerabilities. This could result in significant security volatility and novel types of supply-chain attacks as these systems are deployed and used."***

Taking Action

Learn what AI is and how it works. A basic understanding of the technology is essential to evaluating AI-related cybersecurity and privacy risks and developing effective governance. Because AI capabilities are evolving so rapidly, set aside time on a regular basis to stay updated. With each new development, consider how cybercriminals might find new ways to leverage AI and what new privacy risks could be introduced.

Get ahead of technical debt. With limited time and budget, data governance systems are not always as robust as they need to be. Because the proliferation of AI has been so rapid and is expected to continue in the coming years, professionals who are building AI governance today can't afford to cut corners. As one panelist asked, "If we fail, will we ever be able to put the genie back in the bottle?"

Build AI governance into existing institutional governance. Leverage guiding principles that have already been agreed on and reflect institutional values. Integrate applicable elements from standard industry frameworks, such as the NIST AI Risk Management Framework.

Establish a generative AI safety and security committee. Initially the committee should identify and prioritize risks associated with generative AI adoption. The committee should also be tasked with staying abreast of the rapid developments in AI use, as well as their associated threats.'

Stay informed about evolving legal and compliance frameworks. Officials from a wide range of organizations (e.g., EU, NIST) are creating and revising laws and policies that can impact AI governance at higher education institutions. Incorporate AI cybersecurity and privacy principles into the AI governance model by default, directly supporting compliance with data security, privacy, and regulatory frameworks.

Provide all stakeholders with AI-related cybersecurity and privacy training. Such training should address institution-specific AI governance as well as broader topics such as the ethical and equitable use of AI tools. Include education about why AI governance is crucial to institutional success in order to increase buy-in and compliance.

Collaborate across the institution. Cybersecurity and privacy professionals should be included in relevant working groups across the institution to ensure that cybersecurity and privacy are foundational to all AI-related work. Similarly, cybersecurity and privacy professionals should include colleagues from other units in AI governance work to ensure that other disciplinary considerations and use cases are accounted for.

Take a human-centered approach to AI governance. AI technologies have the potential to expand equity gaps, reinforce systemic inequities, and introduce new barriers for higher education stakeholders. AI governance should include human-centered principles such as the mitigation of bias, the inclusion of humans in decision-making, and constant self-monitoring and improvement cycles.

Build-in continuous improvement to the governance model. AI capabilities, along with their nascency, widespread availability, and broad incorporation into many technology offerings, require a foundational approach to AI governance that will rapidly evolve. Be sure to build continuous revision, policy development, and maturity into the AI governance model for sustainability as AI rapidly evolves, ensuring that your AI governance evolves alongside it.

AI Governance in Practice

Minnesota State Generative Artificial Intelligence Guidelines

Minnesota State developed a comprehensive set of generative AI guidelines to support the operations of its 33 institutions and support student success. A multidivisional team of professionals established three overarching goals for the document: clarify the applicability of existing policies and procedures; provide recommendations and best practices for the acceptable use of generative AI services; and provide a foundation upon which campuses can build local policy.

Implementing Generative AI Policies in Higher Education: The K-State Model

Kansas State University developed an AI governance policy through collaboration with campus offices such as Central IT, Faculty Senate, and General Counsel. This project, designed to comply with Kansas public records laws and federal statutes, categorizes usage into Classroom Use, Research, and Administrative Records. It serves as a model for other institutions, providing actionable guidance for generative AI use while informing broader AI discussions within Kansas and peer institutions.

High-Level Approval Process for the Use of AI Solutions

NC State University includes AI solutions in its IT Purchase Compliance process. The Security and Compliance team developed a simple three-by-three risk matrix, allowing data stewards to review the solution and use case and then approve or deny the request. This matrix measures data sensitivity (impact) by the relationship of vendors to the university (likelihood). This process is intended to curb the use of unsanctioned solutions with no oversight.

Privacy Governance

Among institutions that have addressed privacy governance at all, most fold it into IT security governance or data governance mechanisms. However, privacy—and AI impacts on privacy—presents unique challenges to institutions and should have a strong governance structure. At UC San Diego, we have developed a privacy governance structure that taps into all parts of the organization and leadership.

Data Governance Leads AI Governance at Wichita State University

Because of lingering questions surrounding generative AI, Wichita State University utilizes its data governance process to regulate what data types are allowed to be input into generative AI. WSU relies on the Data Management Committee and sensitivity levels to define when an external data transfer, including to AI, needs to be reviewed prior to the transfer. The review weighs the risks involved against the need for the tool.

RIT: Ensuring Safety and Security of GenAI Adoption

Rochester Institute of Technology (RIT) chartered an Artificial Intelligence Safety and Security Advisory Committee (AISSAC) to examine safety and security risks associated with deployment and operationalization of generative artificial intelligence (GenAI) technologies. This cross-functional committee will identify and prioritize risks associated with these new AI technologies. AISSAC will provide recommendations on mitigating these risks to ensure the safety and security of RIT data, operations, and the RIT community.

FURTHER READING

MIT Technology Review
"Let's Not Make the Same Mistakes with AI that We Made with Social Media"

ISACA
"The AI Reality: New Research from ISACA Identifies Gaps in AI Knowledge Training and Policies"

NIST
AI Risk Management Framework

European Commission
AI Act

European Commission
"Implementing AI Governance: from Framework to Practice"

White & Case
"AI Watch: Global Regulatory Tracker"

The White House
Algorithmic Discrimination Protections

Barracuda
"How Attackers Weaponize Generative AI through Data Poisoning and Manipulation"

IAPP
"What AI Governance Leaders are Thinking About"

SUPPORTING AGENCY, TRUST, TRANSPARENCY, AND INVOLVEMENT

Overview

In our increasingly autonomous digital world, cybersecurity and data privacy can only be protected when individuals are fully informed and empowered. For example, some regulatory landscapes, including that of the United States, require individual subjects to take action such as opting out and requesting deletion to protect their own privacy. By supporting agency, trust, transparency, and involvement, cybersecurity and privacy professionals can go beyond the minimal requirement to give users an opportunity to opt out. Ultimately, practices that center end users' attitudes and needs foster a positive relationship between users and technology, reduce resistance to change, and improve the safety and success of adoption. At the institutional level, supporting agency, trust, transparency, and involvement leads to a healthier and safer organization by bolstering inclusivity and equity. Further, by setting and managing expectations inherently in processes, institutions will be able to build more genuine partnerships with their constituents and partners.

> ***"Providing users with control and encouraging involvement ensures that diverse perspectives are included in the decision-making process, fostering a more inclusive environment."***

Although supporting agency, trust, transparency, and involvement brings many benefits, some risks are incurred as well. For example, cybersecurity and privacy policies and practices that are created to educate users and give them more autonomy also tend to create more work for everyone involved, as well as additional delays in the availability of a service. At a time when higher education staff, faculty, and students are already stretched thin, too much complexity might lead to complacency, confusion, and fatigue. Additionally, too much transparency can lead to unwanted attention, increasing an institution's attack surface and even helping attackers identify vectors into an organization. To mitigate these risks, cybersecurity and privacy professionals should implement continuous cycles of evaluation and improvement.

> ***"Striking a balance between transparency and security, ensuring equitable involvement, and managing the operational burden are key to successfully implementing these practices without introducing additional vulnerabilities."***

Taking Action

Create a standing privacy advisory group. The group should comprise key data-subject representatives (e.g., students, faculty, staff) from a wide swath of your user base. Considering data subjects' understanding of technology, attitudes, and needs when developing new processes, practices, tools, and systems fosters a positive relationship between user and technology.

Communicate with users regularly. Involve users in the design of the transparency/control features. Keep users updated on changes to policies and standards, and empower them to provide feedback. Inform users when their feedback is implemented to encourage further feedback cycles. Use plain language when communicating with users so your message isn't lost in technical jargon.

Provide users with the ability to track their institutional data. Users should know which institutional offices have access to personal data and how those offices use personal data. Users should also know what specific data each institutional office has access to.

> ***"If stakeholders have a sense of safety and control over their data, they'll be more likely to engage with InfoSec, leading to trust and increased involvement."***

Create or revise professional development resources for cybersecurity and privacy professionals. In order to effectively support agency, trust, transparency, and involvement, cybersecurity and privacy professionals need continuing professional development, especially as digital tools and data uses evolve and as regulatory landscapes become increasingly complex.

Stay balanced. While it's important to involve users in policy development and revision, trying to please everyone is a futile exercise and can expose the institution to additional risk. For example, unrealistic user expectations can lead to loss of trust. Set realistic expectations on how user input will be considered and addressed, even if some recommendations cannot ultimately be incorporated.

> ***"We should be instilling [agency, trust, transparency, and involvement] into the general population because everyone needs to advocate for these things. Until there is significant awareness and societal pressure, these concepts will not be successful at the scale they need to be."***

Supporting Agency, Trust, Transparency, and Involvement in Practice

Cybersecurity Spring 2024

The Information Technology unit at California State University Monterey Bay presented a multidimensional cybersecurity program targeted at CSUMB students to increase their awareness of cybersecurity best practices and involve them in the campus community. This was accomplished through gamification of cybersecurity best practices, a lively in-person panel discussion, and a graphic design contest all called "Cybersecurity Spring 2024."

The Demystification and Enhancement of Information Governance at UNSW

This project aims to improve university-wide awareness, understanding, and implementation of information management at the University of New South Wales by developing a single information governance policy that sets out how UNSW manages data, information, and records in an ethical, legal, and responsible manner. The project comprises two stages: the consolidation of existing policies, and the development of persona-based guidance and communities of practice to support UNSW data.

ASU Data Classification Tool

At Arizona State University, we have launched a tool to make data classification accessible to the everyday user, mitigating risks such as inappropriate classification, regulatory noncompliance, and resource exhaustion. Users answer a series of nontechnical questions about their data, which then produces a brief summary of the data's classification and applicable regulations, simplifying compliance in higher education's complex regulatory landscape. This reduces incorrect classification and helps us maintain compliance while securing sensitive data.

Secure and Privacy-Protecting AI Services at the University of Michigan

With a vision of providing just-in-time generative AI tools to support and augment the innovative work of U-M faculty, staff, and students, we have deployed a suite of GenAI services rooted in four key considerations: privacy, security, accessibility, and equitable access. These considerations are central in system design and configuration, data governance, and contractual terms with third-party service providers, resulting in wide adoption and trust across campus.

McMaster University's Values-Based, Collaborative Approach to AI Governance

Recognizing that generative AI exceeds traditional boundaries of disciplines or administrative areas, officials at McMaster University created a cross-functional AI Advisory Committee, setting priorities for, and receiving recommendations from, flexible Expert Panels. Guided by shared principles, these panels, made up of staff, students, and faculty, lend their expertise to projects, including guidelines and resources. This adaptable approach invites the possibilities of this technology while maintaining clarity on risk and ethics.

FURTHER READING

World Economic Forum
"Digital Trust: Supporting Individual Agency"

Huron
"Shades of Gray: The Evolution of Data Privacy Standards in Higher Education"

Australian Government: Department of Home Affairs
SOCI Act 2018 for Higher Education and Research

Microsoft
"How to Build a Privacy Program the Right Way"

Campus Safety
"Navigating Student Data Privacy in Higher Education"

ISACA
"The Practical Aspect: Privacy Compliance—A Path to Increase Trust in Technology"

NIST
"The Importance of Transparency—Fueling Trust and Security Through Communication"

FOCUSING ON DATA SECURITY RATHER THAN THE PERIMETER

Overview

In recent years, the definition of "perimeter" has evolved beyond the border between an organization and the outside world. In fact, some panelists asserted that attempting to define the perimeter in our digital world, which relies heavily on cloud services and third-party software, is all but impossible. Users no longer sit behind institutional firewalls, and attack techniques have pivoted to focus on individual users, their identities, and their credentials. Though protecting the institution's perimeter is still important, focusing on an ill-defined or shifting perimeter opens an institution to a false sense of security. Regardless of where or how an institution's data are stored, they must be protected. Reliance on vendor third- and fourth-party processors of data, especially in light of the recent explosion of AI capabilities offered by vendors, requires a different view of individual and institutional control with respect to personal data. A robust, proactive third-party vendor management perspective and capability are now fundamental requirements for most organizations' data security and privacy programs. For these reasons, today's cybersecurity and privacy professionals must take a data-first approach and focus on data security.

> ***"How do you define the perimeter for [an institution]? Data are kept on premise, in private clouds, and by third parties. Your potential adversaries may also include individuals within a traditional perimeter."***

A data-focused approach to cybersecurity and data privacy comes with some risks. Users could be confused by security measures that follow them beyond the traditional boundaries of their campus and might even feel that their privacy is being compromised or they are being surveilled. User education should be a key component of any effort to increase focus on data security, hopefully increasing user satisfaction and compliance. It's also possible to focus attention and resources too much on data security, neglecting other important elements such as the perimeter. Classic models of security should not be discarded but rather balanced with data-centered processes.

> ***"This is really a 'both and' kind of problem. We should focus on data security but not in place of focusing on the perimeter. It is important to maintain our historical perimeter defenses at the same time that we are working to build-out data-based protections."***

Taking Action

Maintain effective data classification and governance practices. Maintain a data inventory and consistently apply creation, storage, transfer, and deletion practices. Keep data encrypted, and mask or anonymize data as appropriate. Destroy data upon the completion of its life cycle.

Take an inventory of your systems. Identify what data are stored, create maps of data being transferred, and look for ways to reduce your number of systems and transfers to reduce the overall attack surface.

Adopt Zero Trust. Continuously verify and authenticate users, and limit access to only the data users need. Assume that your data have already been breached, leveraging microsegmentation to minimize impact. Ensure that every device that connects to your network is compliant with data governance policies. Always ask yourself what you trust and why, and transition to a default of Zero Trust.

Use data loss prevention (DLP) tools. Such tools enable you to monitor data collection, storage, usage, and loss. DLP tools help ensure that confidential and private information is identified and its egress from the institution is defined and controlled.

Manage users' identities with identity lifecycle management (ILM). ILM includes steps for onboarding users, authentication and authorization, identity and role management, offboarding, and reporting.

Prioritize high-risk platforms, products, and services. Use a classification system to identify the highest areas of risk and invest team resources in these areas first.

> ***"Know what is important; you can't protect everything."***

Focusing on Data Security Rather Than the Perimeter in Practice

SDSU Secure Enclave

San Diego State University, using AWS, has created a Secure Enclave platform for research. This platform ensures secure environments for handling regulated data, meeting IT security compliance, and maintaining NIST 800-171 controls and strict enclave separation. It provides managed services for data ingress/egress, logging, and deployments; supports standardized system images; and allows automated tool deployments and future service additions to meet evolving researcher needs.

Reducing Exposure in OneDrive by Tightening Permissions

After close to a decade of campus usage of OneDrive at Ball State University, stale permissions and permissions sprawl have created an environment in which ensuring that university data are safeguarded is difficult. While cloud services have created both opportunity and convenience, the implementation of such services has increased the necessity for strengthening user rights due to the lack of a physical perimeter.

FURTHER READING

ISACA
"Identity as a New Security Perimeter"

Transforming Data with Intelligence
"Data Security Posture Management in the Education Sector: What You Need to Know"

Seclore
"Securing Data Beyond the Perimeter: Why DLPs and Firewalls Aren't Enough Anymore"

Aberdeen
"Making the Shift from Perimeter to Data Security"

NIST
Cybersecurity Framework

Apogee
"The Zero Trust Model in Higher Education—A Necessary Shift"

Twingate
"Shifting Paradigms: From Perimeter Defense and VPNs to Zero Trust Security"

ENISA
"Foresight Cybersecurity Threats For 2030—Update 2024: Extended Report"

AI-ENABLED WORKFORCE EXPANSION

Overview

The recent explosion in generative AI technologies has already impacted or will soon impact a significant portion of the workforce, especially in the global north. Higher education cybersecurity and privacy professions are no exception to this revolution, and panelists posit that AI will actually enable workforce expansion in their fields. Both new and veteran cybersecurity and privacy staff could be supported by emerging AI-powered tools. For example, staff can use personalized and adaptive training tools to upskill more effectively and efficiently, lowering the barrier to entry and increasing retention. Staff can also use AI-powered tools to augment their completion of routine tasks such as threat detection, anomaly detection, and incident response, allowing staff to handle a larger volume of work with lower error rates.

> ***"AI adoption is becoming ubiquitous within most industries, and with InfoSec it is fueling faster detections, investigations, and responses to both defenders and attackers."***

Notably, the panel was not unanimously convinced that AI tools will enable the expansion of the cybersecurity and privacy workforce in higher education. One panelist cautioned, "[AI] could lead to more skills required, not less, as new employees need to understand AI and data science on top of their other required skills." In this way, AI may impact the future of the cybersecurity and privacy workforce by both supporting them to accomplish some tasks and requiring them to upskill for others. Indeed, panelists agreed that new skills will be needed, at the very least to understand and respond to increasingly advanced AI-enabled cyberattacks.

> ***"If we fail to arm our cybersecurity and privacy professionals with AI-enabled tools, it will be like sending them to a gunfight with a toothbrush. The power of AI in the hands of the bad actors cannot be underestimated."***

Taking Action

Don't forget the value of human intuition, creativity, and insight. As one panelist explained, "Cybersecurity and data privacy still have a lot of art, history, and institutional knowledge skill requirements." An overreliance on technology solutions of any kind could lead to increased attacks and failure, weakening the institution overall.

> ***"I am a huge advocate for strengthening our workforce's command of the humanities. This will provide them with ethical and critical-thinking toolsets that will be imperative to our successful future."***

Be aware of AI's limitations and flaws. A major risk in adopting AI-powered tools for any job is the potential introduction of new and worse errors than what is expected from human work. Often such issues arise because users of AI tools do not understand how the technology works, leading to a false sense of trust in outputs.

Routinely evaluate where and how AI-powered tools can be deployed. Ideally, such review would come from a diverse committee comprising staff from cybersecurity, privacy, and other relevant units such as HR and IT. Because AI technologies evolve so rapidly, committee members should also continuously reevaluate their recommendations.

Implement policies or guidelines for using AI-powered tools for work. AI governance should align with other institutional and unit-level frameworks. Further, policies or guidelines should be in place before any tool adoption and should include processes for humans to validate AI outputs.

> ***"There are already many concerns around unethical uses of AI and worker displacement... Refer back to agency, trust, transparency, and engagement."***

Carefully select tools that include AI technology. Be sure to consider the total cost of ownership so that you don't lose time and money learning and managing tools, negating any boost to the efficiency of other tasks. Monitor AI-powered tools even after adoption; changes in the tools' capabilities and processes might lead you to discontinue use at any time.

AI-Enabled Workforce Expansion in Practice

AI Penetration Testing

Comprehensive visibility into the cybersecurity threat landscape is essential to mitigating data loss and privacy risks. Human-led penetration testing has limits, including the number of tests per year and inconsistent quality of results. AI penetration testing offers significant advantages in testing frequency, consistency in the quality of results, and discovery of security weaknesses in the environment. At Clark University, by combining human-led and AI-led penetration testing, we achieve maximum visibility into our threat landscape.

AI Malicious Email Mitigation

Social engineering is a prominent breach vector by malicious actors. A common social engineering vector is through institutional email targets as phishing attacks. One approach to limiting this risk is to operate a malicious email reporting program managed by security personnel. However, such programs siphon valuable time away from constrained infosec teams. At Clark University, by leveraging AI-powered malicious email mitigation tools, engineering resources can be redirected while improving security posture.

AI-Generated Web Crawler for Institutional Domain Keyword Searching

This web crawler was created at Miami University (Ohio) in response to the recent polyfill.io service vulnerability allowing malicious code injections. The web crawler will search for keywords such as polyfill.io, limited by the base domain to prevent searching content outside our university, with added features to identify pages containing broken links or links that are not secure. The Python script was initially generated by ChatGPT and refined by security analysts.

FURTHER READING

Employment Transition Solutions
"Harnessing the Power of AI LLMs in the Workplace"

Mark Williams
"The Role of AI in Reshaping Leadership in 2023"

MIT Sloan Management Review
"How HR Leaders Are Preparing for the AI-Enabled Workforce"

Harvard Business Review
"How AI Can Make Us Better Leaders"

McKinsey Global Institute
Generative AI and the Future of Work in America

Forbes
"The Future of the Cybersecurity Profession with the Rise of AI"

PRIVACY-ENHANCING TECHNOLOGIES

Overview

In the face of rising cybersecurity and privacy concerns, including increasingly sophisticated threats and attacks, cybersecurity and privacy professionals are leveraging privacy-enhancing technologies (PETs). PETs help organizations use data to make decisions or offer services while improving privacy compliance, ethics, and trust with stakeholders. PETs often use data collection and processing practices to anonymize or limit exposure of personally identifiable information (PII) by design. PETs can be used to protect privacy, for example, through federated learning, keeping more PII in an individual's control (e.g., on a person's mobile device). The PII is not shared to a data set or model that could be further shared with others publicly. Another example is differential privacy, which allows organizations to share trends within a data set while obfuscating individual's records in the data set. It's important to note that these methods can provide varying levels of protection and are not foolproof, often requiring expert knowledge. PETs may not offer full guarantees of privacy and often involve tradeoff decisions of data usability and quality versus privacy.

> ***"PETs will be key to putting cybersecurity and, in particular, privacy professionals in the forefront in framing organizations' strategic investments around privacy compliance and user privacy."***

PETs are just one element of a data-centered approach to cybersecurity and privacy. After minimizing the volume and sensitivity of data stored at an institution, PETs add an extra layer of security to the data that remain. When used properly, PETs can obfuscate data while still enabling users to analyze the data, supporting critical institutional functions such as research and learning analytics. However, all technologies present at least some risk. Adding PETs to an institution's existing cybersecurity and privacy strategy could introduce additional complexity and increase the demand for operational overhead and other resources. PETs are not foolproof; they can be misconfigured or misused. Systems and tools must be continuously monitored and validated. Even when implemented properly, PETs can also introduce a false sense of security among users, leading to relaxed data-minimization processes.

> ***"Privacy and security often go hand in hand. As we defend people's privacy, we typically lessen the amount we have to secure."***

Taking Action

Don't overestimate the power of PETs. One panelist explained, "Privacy is much more than technology. Rather, privacy is a personal, social, cultural, and political construct requiring a multidisciplinary approach." PETs do not address the core issues of human-created systems and processes, so cybersecurity and privacy professionals must remain vigilant in a holistic approach to their work.

Ensure the ongoing management of PETs. These technologies are designed to run with little human involvement, but as the institution's data landscape changes over time, cybersecurity and privacy professionals need to continuously monitor their efficacy. If a PET is compromised, the data it is designed to protect may be compromised as well. Create policies and procedures to ensure the ongoing management of PETs.

Stay mindful of data quality. With PETs in place, users and even cybersecurity and privacy professionals might not be able to see how data are used, accessed, and shared. This lack of insight raises concerns about data quality and can negate steps aiming to support trust, agency, transparency, and involvement.

Provide users with adequate training. Because PETs are not currently widely adopted, users may not understand what they are or how they work. Users will need training, especially if they are to understand the limitations of PETs and mitigate the introduction of more risks to cybersecurity and privacy. For example, users should be provided with data literacy training so they understand the functions of PETs that rely on statistical processes.

> ***"Privacy technology is one tool of many to help address real inequalities in privacy and power across the world."***

Be strategic. Continue to leverage existing technologies while you research new PET options. Carefully evaluate where PETs can and should be applied, and work with software development and project management teams to embed PETs into current and future projects.

FURTHER READING

ISACA
"Exploring Practical Considerations and Applications for Privacy Enhancing Technologies"

NIST
"Differential Privacy for Privacy-Preserving Data Analysis: An Introduction to our Blog Series"

Brookings
"Using Differential Privacy to Harness Big Data and Preserve Privacy"

Clearcode
"The Benefits of Privacy-Enhancing Technologies (PETs) in AdTech"

Springer Link Encyclopedia of Database Systems
Privacy-Enhancing Technologies

The White House
"Advancing a Vision for Privacy-Enhancing Technologies"

Federal Trade Commission
"Keeping Your Privacy Enhancing Technology (PET) Promises"

Georgetown University, Massive Data Institute
"Privacy-Enhancing Technologies: Guiding Educators on Sharing and Protecting Student Data"

Privacy Enhancing Technologies Symposium
Proceedings on Privacy Enhancing Technologies Symposium

World Economic Forum
"The Impact of Privacy-Enhancing Technologies (PETs) on Business, Individuals and Society"

The Organisation for Economic Co-operation and Development (OECD)
Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches

AI-SUPPORTED CYBERSECURITY TRAINING

Overview

Across higher education units, from teaching and learning to business operations, stakeholders are seeing more and more opportunities to leverage AI to create personalized learning experiences. Certainly, personalized learning powered by AI is not particularly new. However, the recent, rapid advancement of generative AI has renewed interest in using AI of all types to enhance learning experiences. Arguably, one of the most challenging parts of working in cybersecurity or privacy at a higher education institution is developing and deploying training for all institutional stakeholders—faculty, staff, and students. AI-supported cybersecurity training may enable the creation of more-focused, role-specific cybersecurity training for users in higher education. Beyond creating personalized learning experiences, AI can also be used to improve users' engagement in training. For example, real-world cybersecurity scenarios can be simulated, providing users with hands-on practice in a controlled environment.

> ***"AI-enabled cybersecurity training is the next frontier [because] it offers the ability to impart personalized learning experiences tailored to individual needs and preferences by providing real-time feedback and identifying knowledge gaps for targeted improvement."***

Meanwhile, interest in using AI for the work of instructional design, including cybersecurity training, is increasingly widespread. Training designers can leverage AI to analyze internal cybersecurity incidents, integrate insights from other institutions' experiences, and prioritize training topics according to risk profiles. Exciting opportunities are emerging to improve training in the coming years, but some concerns remain. For example, without proper human oversight, AI-powered training tools could mislead users, reinforce practices that don't work, or even hallucinate incorrect information. Potential consequences extend beyond the institution. For example, experts warn that the environmental impact of training LLMs, using LLMs, and constructing and running data centers is creating significant setbacks in sustainability goal progress for technology companies. As with all technology adoption, institutional stakeholders will need to carefully examine the benefits of AI-supported cybersecurity training and weigh them against potential risks.

> ***"Phishing simulations, tabletop exercises, and simulated attacks on infrastructure are all areas that could benefit from the inclusion of AI-enhanced training."***

Taking Action

Collaborate with colleagues to determine best practices. Because this is an emerging capability for most institutions, no standard playbook exists for how institutions can or should integrate AI into professional development. Cybersecurity and privacy professionals will need to work together to create one.

> ***"AI tools can make training more accessible by accommodating different learning [needs], formats, and languages."***

Evaluate new AI-supported cybersecurity training. To get the most out of your training, create measurable goals, choose curricula that are aligned with those goals, and then collect data to find what works and what doesn't.

Track trends and identify emerging tools. AI is currently evolving exponentially, new tools are continually available. Of course "new" does not always mean "good," so novel tools will need to be researched and vetted. Some tangible ways you can keep an eye on trends and emerging tools are to join AI-related professional development groups, subscribe to AI newsletters, and connect with AI professionals on professional networking platforms.

Look for opportunities to implement positive change. AI-powered training tools might provide completely new options for training users, but you might encounter resistance from some stakeholders who hesitate to depart from established processes and products. Lean on best practices from change management experts (e.g., understanding and including users in change processes) as you shift your training approach.

Embrace a mindset shift toward how AI can be leveraged to support your institution. It can be tempting to focus on the many risks AI technologies introduce to institutions. Though keeping risks in mind is important, balancing risk and opportunity can help institutions integrate AI solutions for improved efficiency and efficacy.

Collaborate with teaching and learning colleagues. Working with colleagues who have deep expertise in teaching and learning, instructional design, and educational technology will help you create pedagogically sound training materials and programs.

Protect your relationship with users. At some institutions, high-touch training programs are one of the few ways cybersecurity and privacy professionals are able to engage with users. Adopting more computerized training may decrease the number of opportunities to engage with the community. Protect your relationships with users by maintaining engagement with them, perhaps through Q&A sessions and alternative training options for those who do not enjoy computerized training.

AI-Supported Cybersecurity Training in Practice

Framework for Upskilling CSU IT Workers in CompTIA Security+

California State University Channel Islands employs experienced staff, but very few have industry certifications. We wanted to spur employees to focus on getting trained and attaining certifications. We conducted a three-month training twice a week and had such a good experience that we ran the training a second time, this time with student workers. With the help of AI, we were able to craft a cybersecurity training program and get several team members CompTIA Sec+ certified.

AI-Supported Cybersecurity Training Using NIST Work Roles and NCAE-C Standards: Personalized Learning Pathways

CyberEd in a Box merges academic learning with industry mentorship, using AI to rapidly prepare individuals for cybersecurity careers. Funded by NCAE-C and centered at Norwich University, with support from the Careers Preparation National Center, the program offers certifications, apprenticeships, and practical experiences. It uses AI for personalized learning paths, competency assessments, and continuous support, emphasizing moral character development and creating a strong pipeline of skilled cybersecurity professionals with a significant community impact. The University of Washington and the University of Hawaii have been early adopters of this approach.

AI Safety for Students

Developed by industry leaders KnowBe4 and Synthesia, this module provides students with an understanding of AI. Using KnowBe4's cybersecurity expertise and Synthesia's AI-driven video technology, students explore AI fundamentals, applications, and evolving role in daily life. They gain essential knowledge and skills to navigate the digital world safely while leveraging AI capabilities for educational and entertainment purposes, preparing them to make informed decisions in an AI-enhanced environment.

Cybersecurity and You: AI-Enhanced Training Module for Students

At the University of Illinois, we used generative AI while developing an interactive module that covers protecting accounts and devices, recognizing phishing, and using social media safely. Some unique features include using AI-generated art to visualize complex passphrases and a "choose your own adventure" story on a lunar base. The module integrates into existing courses, providing skills to help students navigate online risks and enhance their digital literacy and safety.

FURTHER READING

Cyber Security Review
"The Impact of AI on Cybersecurity Awareness Training"

EC-Council University
"The Role of AI in Cybersecurity – A Comprehensive Guide on AI in Cybersecurity"

Fortra
"How Artificial Intelligence Benefits Cyber Security Awareness Training"

2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)
"AI-Driven Customized Cyber Security Training and Awareness"

University of Cincinnati Online
"How Instructional Designers Use AI to Optimize Workflow and the Learning Experience"

Association for Talent Development
"Harnessing the Power of AI in Training and Development"

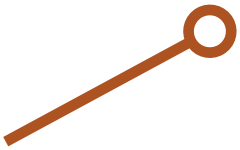
SCENARIOS

With the trends we're observing and the technologies and practices emerging around us that are already helping shape the future, we can begin to imagine how all of these elements might combine and coalesce into larger stories about who we'll be as people and what higher education will be in the future. In this section, we offer several of these larger stories through a series of scenarios that reflect on where these trends and technologies and practices may ultimately lead us in 10 years' time.

To paint these scenarios, we used a forecasting framework from the Institute for the Future (IFTF) to envision four distinct possible futures that each takes a different angle on how today might be leading into tomorrow. The first scenario we envision is characterized as Growth, a scenario in which the current trajectories of things today have continued along their same paths into the future, breaking past previous limits. The second scenario is Constraint, a scenario in which higher education has organized itself around a common threat or core guiding value or principle that drives our decision-making and animates our daily practices. In the third scenario, Collapse, we imagine a future in which higher education has experienced a series of breakdowns and widespread changes that ultimately leave many institutions decimated due to a failure of human systems to overcome inherent tensions or weaknesses. In the Transformation scenario, a new paradigm has been established within higher education that has led to a fundamental shift in the ways we think about and carry out education, stretching our imaginations and challenging our assumptions.

Panelists were actively engaged in creating the scenarios through small-group discussions imagining first-, second-, and third-order consequences for several possible futures that built on some initial sketches. For Growth, panelists explored implications of a future where institutions prioritize spending on cybersecurity and privacy over key institutional operations. In the Constraint scenario, governments across the world create a central identity verification system. The potential future for Collapse was a world where political strife leads to internet fragmentation and the end of the World Wide Web as we know it today. And finally, in the Transformation scenario, educators teach learners of all ages about cybersecurity and data privacy.

The scenarios we offer here represent only potential futures, of course. With so much changing around us seemingly on a daily basis, it is impossible to know with any degree of certainty who we'll be and what higher education will be in 2034. Scenario exercises like these help us anticipate and plan for our future, grounded in the best information we have available to us, so that we can be more prepared to face whatever future does eventually arrive.



Growth

Collapse

Constraint

Transformation

GROWTH: SKYROCKETING FUNDING FOR CYBERSECURITY AND PRIVACY

Data Health Support as a Selling Point

A small cluster of prospective students and their parents ambles across the wooded lawn of a northwestern university, coming to a stop in front of an angular glass-and-metal building. Its five-story walls jut above the encircling pines in a mosaic display of shapes and patterns, a modern architectural marvel standing out from an otherwise traditional red-brick campus.

"Some of you were asking earlier about your students' data health and safety," the group's tour guide says, motioning proudly at the building. "This is the Dorothy E. Denning Center for Data Wellness, which was opened just last year through a very generous $550 million endowment."

The guide pauses for dramatic effect as visible amazement ripples across the group. One parent in the back of the group nudges their kid, eyes wide as if to say, "Wow!"

"With this endowment," the guide continues, "our school is poised to be at the forefront of modern data wellness practices and innovations. We have some of the world's best cybercrime professionals and data physicians working here in the center, so your students will not only have access to world-class learning and work-placement opportunities, but they'll also be completely data-fit while they're under our protective care."

The guide takes out a phone and holds it aloft. "But don't just take my word for it. If everyone can pull up your data fitness apps, you'll see that we've already been cleaning and strengthening your personal data health even in the short time since you've arrived on campus."

A prospective student eagerly opens the data fitness app on her phone and is immediately greeted with the "ding!" of a notification. "You have ten resolved data health issues," the notification reads. She navigates to the summary dashboard in her app where the needle on a small meter jumps all the way to the right, indicating full data health. "You are at maximum data fitness," a header at the top of the dashboard reads.

"Now," the guide interjects, "I don't do this for all my tours, but if you'd like to get a peek inside the center, we can make up the time by skipping a few of the other stops on the tour."

The group voices its approval and makes its way down the short path to the large glass entryway to the center's lobby.

Forced to choose between better cybersecurity and business as usual, higher education institutions prioritize cybersecurity and privacy funding. There seems to be no limit on what institutions will spend on cybersecurity and privacy, but budgets for key institutional operations continue to dwindle.

How Did We Get Here?

Following the rapid advancement of generative AI in the early 2020s, higher education institutions experienced a severe increase in the frequency and sophistication of cyberattacks. With the help of generative AI tools and the expansion of institutional perimeters, bad actors were finding easy ways to breach institutions through end users, especially students. Several notable cases made international headlines. In one landmark case, a large, research-intensive institution not only lost millions of dollars in a series of attacks, it also lost students and faculty due to loss of community trust. Additionally, a significant number of smaller institutions have closed due to ransomware attacks that they couldn't recover from. In response to the alarming uptick in cybercrime, losses in revenue, and heavy fines, many institutions chose to divert limited budgets and significantly increase spending for data governance that protects cybersecurity and data privacy.

Higher education institutions are enjoying many benefits from their increased data governance spending. Most institutions now have established data governance bodies, with clearly defined roles and responsibilities. Data across the institution are more integrated and more effectively managed. Data are more available for stakeholders who need them for vital operations such as research, institutional decision-making, and learning analytics. Users create custom AI assistants trained with granular data to inform their work. Administrative workflows are more efficient and do not need as much human capital to function. Benchmarking across institutions is easier, strengthening higher education's commitment to collaboration and data-informed decision-making.

As institutions' data governance structures have become more robust, so too have the staffing levels and the breadth of cybersecurity and privacy professionals, such as legal experts and privacy consultants. As a result, institutions are more compliant with cybersecurity and privacy regulations and frameworks (e.g., GLBA, NIST). Colleges and universities suffer drastically fewer breaches, bolstering users' trust in their institutions. And as users have more trust in their institutions' collection and use of data, they are more willing to share personal data, adding to the boost institutions are seeing in research and analytics capabilities.

Though many higher education leaders predicted and hoped that shifts in budgeting would eventually equilibrate with little to no impact on institutional operations, institutions have actually experienced profound changes to core teaching and learning capabilities. For most institutions, funding was diverted away from critical teaching and learning budget items, such as support for instructional design, teaching assistants, and educational technology. With insufficient funding, some degree and certification programs had to close down. Institutions increased tuition to make up for these budgetary shortfalls, but it was impossible to close revenue gaps through tuition because any increase catalyzed already declining enrollments. Because programs have spent the past 10 years fighting for funding, cybersecurity and data privacy budgeting have now become a dividing issue. Some stakeholders see it as a strategic investment, while others see it as a waste of money that should be used for more direct student services. With limited ability to recruit students based on previous offerings such as extra- and cocurricular support, institutions are leveraging their strong cybersecurity and privacy stances as selling points. Our community is wondering whether this cybersecurity and "privacy first" stance is the new normal.

COLLAPSE: THE END OF THE WORLD WIDE WEB

New Barriers for Scholarly Collaboration

[message dated: July 21, 2035, 09:10am]

Hello, Dr. Silva. It was a pleasure meeting you at the conference in São Paulo last week. As we discussed, I'm very interested in your research on three-dimensional string-nets and would love to set up a time to chat more about how my recent work on neutrino interactions might help advance the work you're doing. Just let me know if you have some availability for a call next week and I will send over an invite.

Best - Darnisha Evans, PhD

[message dated: August 12, 2035, 14:35pm]

Greetings, Dr. Evans. I apologize for the delay in my response. It appears your message was sent to my spam folder, I'm assuming due to some recent changes in our permissions with international email communications. It may be easier to correspond through our personal email, as global email platforms tend to be easier for these sorts of things. My personal email is ~~<redacted>~~.

Otherwise, I should have some availability next Tuesday at 2pm your time. I look forward to receiving your invite!

Dr. Lucas Silva

[message dated: August 17, 2035, 15:15pm]

Hi, Lucas. Your personal email address was redacted from your message, likely due to your new communication restrictions and filters (or possibly due to mine). I've attempted several times to forward you a meeting invite, but I keep receiving delivery failure notifications.

I'll just add the Zoom link here, which you can use for our meeting tomorrow: ~~<redacted>~~

Darnisha

[message dated: August 18, 2035, 08:01am]

Greetings, Darnisha. The Zoom link you provided was redacted as well, likely due to ~~<redacted>~~. I wonder if ~~<redacted>~~ might be more effective for communicating from here on out, in which case you can find me at ~~<redacted>~~.

Here's hoping we can connect soon - I really do believe there's great potential between our two bodies of research!

Lucas

[message dated: August 18, 2035, 09:00am]

VIOLATION NOTICE: Your recent messages to "devans@state.edu" have been flagged as violations of communication restriction 13.b.1 prohibiting the international exchange of information that is of a sensitive nature and/or of national interest. Communications to "devans@state.edu" have been restricted for the next 90 days, after which messages will be subject to additional monitoring and restrictions as needed.

[message dated: August 18, 2035, 10:15am]

~~<redacted>~~

Political leaders all over the world admit defeat in the global war on cybercrime. Unable to agree on ways to protect citizens and governments, allied nations create border firewalls, segmenting the global internet according to political alliances.

How Did We Get Here?

The widespread political conflict, increasing hypernationalism and authoritarianism, and rising politically motivated cyberattacks of the early 2020s caused political leaders around the world to re-evaluate the costs and benefits of a World Wide Web. In 2025, political leaders from around the world held a series of international summits to simplify and integrate the global landscape of cybersecurity and privacy regulations in an effort to make the global internet safe for all users. After more than a year of debate, summit participants were not able to reach any consensus. Instead, leaders chose to implement border firewalls, restricting connectivity to citizens and allied nations. As a result, there is no longer a global internet.

The fragmentation of the internet has had widespread impacts on nearly every facet of life. Although international cybercrime has seen a significant reduction, few internet users believe that the benefits outweigh the costs. Societies are more isolated than ever, strengthening echo chambers of thought and culture that reinforce hypernationalism and xenophobia. Authoritarian leaders have flourished in this environment, at the cost of escalating hate crime and decreasing immigration.

The economic impacts of border firewalls have been staggering. Multinational corporations and commercial partners can only use digital tools approved by all relevant governing bodies. Global commerce has been severely impeded, generally prohibiting a large proportion of international sales. Global supply chains are much slower since they are so severely restricted. Workforce growth has been stifled because companies cannot easily recruit globally. With less diversity in regional workforces, idea generation and innovation have slowed. Without international subcontracting, operational costs are rising. Governments are scrambling to keep up with this newly fragmented global economy, implementing safeguards to prevent recession, but economists warn that without reinstating global digital communication, we will continue to face economic decline.

Similarly, higher education institutions are struggling to maintain operations consistent with their core values and missions. Multinational institutions are typically not able to operate cohesively and have had to reorganize their physical locations and resources to match their new digital borders. Institutions are also not able to recruit students as effectively across borders, so all institutions are facing drops in international enrollment and increases in domestic enrollment. For those that previously relied on sizable tuition income from international enrollment, these changes have been all but devastating. And perhaps more impactful than financial consequences, the loss of diversity among people is creating a loss of thought diversity, further exacerbating the issues at hand. The higher education workforce has been similarly impacted, losing the ability to recruit faculty and staff from all over the world. International research collaborations have also been stifled, particularly with respect to research that addresses global challenges such as climate change and international affairs. Altogether, the higher education community is worried that without reinstatement of the World Wide Web, we will never get back to being a global community.

CONSTRAINT: SACRIFICING PRIVACY FOR SECURITY

Tracking and Monitoring Student Data Practices

"Here comes the morning rush," Dannie mutters as he sets down his coffee and stands to greet the influx of students arriving for the day's classes. He motions to the student nearest to his kiosk.

"Step on up," Dannie says to the student. "Set your phone and any wearables you have on the scanner, and let me see your computer, please."

The student sets a phone, watch, and pair of digital glasses on a small flat surface that flashes green once it registers the devices. Dannie takes the student's laptop and connects it to a small cable running to a monitor on a table behind the kiosk. The monitor blips awake to a screen of the school's mascot—a cartoonish old miner wearing a hard hat and wielding a pickaxe—tapping his foot and staring at a wristwatch. "Scanning" blinks in and out at the top of the screen.

"Since your last scan, have any of these devices been in the possession of another person for an extended period of time, even a friend or a family member?" Dannie asks.

"No," the student replies.

"Since your last scan, have you visited any of our prohibited websites or downloaded any of our prohibited apps?" Dannie asks, motioning to a poster on the wall listing the prohibited websites and apps.

"No," the student replies.

Dannie's monitor chirps a quick, happy tune, signaling the completion of its work.

"Your phone and glasses are clean and can be removed from the scanner," Dannie says. "Your watch was flagged as hosting a suspicious anomaly. Do you consent to a digital scrub for your watch now, free of charge? Failing to consent will prohibit you from being able to enter the campus at this time."

"Yes, I consent," the student replies.

Dannie mashes a button on his monitor and the device scanner kicks back on, this time flashing yellow as it removes the watch's impurities. He unplugs the cord from the student's laptop and hands the laptop back to the student.

"You will be on limited internet access for the next 30 days, as you did indeed visit one of our prohibited websites. You're lucky, though, as no anomalies were detected. If you'll stand over there, your watch should be finished scrubbing in just a moment."

The student steps aside, annoyed but resigned.

"Next!" Dannie yells.

Struggling to combat escalating identity theft and fraud, governments work together to implement central identity verification and proofing systems. Independently, stakeholders such as corporations and higher education institutions seek to reduce data footprints by restricting personal device use for employees and students.

How Did We Get Here?

As the rate of technological development increased rapidly in the early 2020s, so did concerns about cybersecurity. In the face of rising identity theft and fraud, cybersecurity leaders and politicians in the United States argued that the only way to protect individuals in a digital world was to implement strict governmental controls through central identity verification. They also urged employers and institutions to limit individuals' use of personal technology in data-rich environments such as work and school. For many, this strategy was (and still is) at odds with a value system centering on autonomy and personal privacy. Eventually, increasing sophistication of cyberattacks forced the government to action. In 2026, the United States joined nations all over the world, signing a five-year plan to implement central identity verification and proofing. Concurrently, companies and organizations began to introduce restrictions for the use of digital devices at school and work in order to shrink both individual and institutional data footprints.

Today's data landscape looks very different from how it did 10 years ago. In 2031, the first worldwide identity federation was instituted as a result of several large international identity federations merging. It is responsible for creating, refining, and enforcing international identity verification standards. Countries are incentivized to opt in to the identity federation for multiple reasons. First, those that maintain their own standards are typically seen as weaker, presenting better targets for cybercrime. Second, safeguarding central identity data is extremely resource-intensive, requiring high levels of expertise and financing. Thus, the worldwide identity federation allows countries to share resources and ensure better cybersecurity.

Tracking which data an individual produces and accesses has never been easier. Further, widespread crackdowns on connecting digital devices to the internet from anywhere except home are reducing the amount of digital information that is created by end users. Our digital environment is still expanding but at a much slower rate than projected 10 years ago, and the digital environment is safer than ever. However, many privacy advocates argue that societies are not doing enough to safeguard individuals' rights. For example, it is nearly impossible to live an "off-grid" life in most countries because central identity verification is required for essentially everything—basic utilities, health care, education, and more. In some places it is illegal to not comply with central ID standards, so anyone who wishes to live off grid must do so in true seclusion.

Higher education institutions have embraced the cybersecurity and privacy changes of the past 10 years. The central identity system has increased the efficiency of higher education operations. For example, hiring processes have been streamlined because prospective employee career experiences are more easily verified. Similarly, student academic records are easier to verify, streamlining complex processes such as institutional transfers. Further, institutions no longer need to maintain their own traditional identity systems, relying instead on the larger central identity system. Institutions have also implemented personal device restrictions on campuses. Not surprisingly, these changes were first met with resistance from students, staff, and faculty alike. However, over the past few years people have generally grown accustomed to compartmentalizing internet access, keeping work at work, learning at school, and personal access at home. The new normal has been uncomfortable, but we remain committed to building a safe digital world.

TRANSFORMATION: ESTABLISHING CYBERSECURITY AND PRIVACY TRAINING AS FOUNDATIONAL CURRICULAR ELEMENTS

Cybersecurity and Privacy Training for Young Learners

"Everyone come to the rug and sit criss-cross applesauce," Mrs. Taylor instructs her kindergarten class. A dozen kids noisily bound over to a rug tucked into a corner of their classroom, each finding a place to sit on one of the small circles dotted across the rug's fabric. "Jackson, put the glue down and come sit," she chides.

From her stool at the front of the rug, Mrs. Taylor opens a book outward to her class so that they can see the illustrations as she reads. "Captain Data-Doodle and the Mischievous Data-Munching Monster," she begins as the kids giggle and fidget.

Slowly turning each page as she reads and scans her eyes across the class, her animated voice rising and falling, Mrs. Taylor narrates the story of Captain Data-Doodle, a heroic dog who teaches kids about the values of data privacy by thwarting the dastardly plans of a rogue gallery of data ne'er-do-wells. In this book's adventure, a data-munching monster terrorizes a small village of squirrels who've failed to properly store and secure their data.

"These squirrels have no locks on their windows and doors, and their passwords are as easy as 1-2-3-4," Mrs. Taylor reads in the booming voice of the data-munching monster.

On the wall behind Mrs. Taylor, posters display various elements of the school's kindergarten curriculum. A math poster illustrates 20 sequential clusters of apples, from one apple to 20 apples. A reading poster shows the alphabet, and another poster just underneath it lists combinations of letters that form simple three-letter words. One poster lists the "Do's and Don'ts" of password protection.

"Do ... use numbers and symbols."

"Don't ... share your passwords with friends."

Another poster features Captain Data-Doodle holding a padlock shield in one paw and a key sword in the other, a blue hero's cape flapping in the wind, and a speech bubble with Captain Data-Doodle's famous catchphrase, "Keep your paws off my data!"

Mrs. Taylor closes the book. "Now, what do you think those squirrels should have been doing to protect their data?" The kids' hands shoot up into the air. Jackson impatiently exclaims, "Eat more glue!" The kids giggle as Mrs. Taylor rolls her eyes.

Recognizing the growing impacts cybersecurity and privacy breaches have on society, educators integrate cybersecurity and privacy training for learners of all ages. Benefits are far-reaching, from educational institutions to the workforce, but some stakeholders are leveraging this training as a new way to gain power.

How Did We Get Here?

The year 2025 was one of the most transformative that the cybersecurity and privacy professions have ever experienced. On the heels of generative AI exploding into public consciousness, a group of previously unknown cybercriminal activists tried to force the public to acknowledge the impacts of big data on the environment. In a series of coordinated cyberattacks, colleges, universities, and AI industry leaders suffered real-world consequences. In one case, a quantum computing research lab's computers were destroyed. In another, an institution's physical plant office was unable to pay any of its staff for nearly a month. Educators realized that cybersecurity and privacy literacy training must be a foundational element of the educational experience, and they began implementing such training throughout K–12, higher education, and beyond.

The initial need for training learners was much greater than schools' capacities to hire new instructors, creating a strong market for third-party providers' AI-powered software. These solutions remain an attractive option because privacy and security laws are only getting more complex, and because AI technology keeps training updated with the ever-evolving legal landscape. AI-powered tools are also personalized and adaptive, even offering just-in-time interventions. Further, third-party solutions tend to be less expensive to scale than in-house programs. The tradeoff is that now large technology companies have a lot of influence over curriculum, a topic of concern for some educators, learners, and families.

Indeed, undergoing massive curriculum reform has not been simple. Local education entities have been creating their own cybersecurity and privacy curriculum standards, and digital education researchers have been publishing national and international standards for cybersecurity and privacy education. Arguments over what should be taught to students of various ages are abundant, and politicians are leveraging differences in opinion on curriculum to divide voters. Experts note that there are lessons to be learned from efforts to expand health literacy in the 1980s and 1990s and IT literacy in the early 2000s, urging educators and communities to work together instead of slowing progress with infighting. So far, social and political influences have made it impossible to standardize curricula, increasing gaps in digital education based on demographics such as age and socioeconomic status.

Despite the challenges educators face, we're already seeing that the near-ubiquitous implementation of cybersecurity and privacy training in education systems is making a positive impact. Training curricula have become more gamified to appeal to younger audiences, and this has increased participation for people of all ages. Students are more interested in broader ethical issues such as democratic values, autonomy, and privacy. Especially in the age of AI, these conversations are vitally important. Students are also more aware of cybersecurity and privacy professions now, and these career paths are seeing a welcome increase in the number and diversity of prospective professionals. What's more, these impacts are starting to extend beyond school walls. As individuals are becoming more aware of the importance of cybersecurity and data privacy, they are beginning to push legislators to improve national policies and regulations. For example, the United States has recently begun earnest work on a cohesive national privacy policy, and there are even talks of a new, expansive Privacy Department housed within the FTC. Educators are leading the way to a safer future.

METHODOLOGY

The Horizon Report methodology is grounded in the perspectives and knowledge of an expert panel of practitioners and thought leaders from around the world who represent the higher education, cybersecurity, privacy, and technology fields. Members of this report's panel were sought for their unique viewpoints, as well as for their contributions and leadership within their respective domains. The panel represents a balance of global contexts. We also sought balances in gender, ethnicity, and institutional size and type. Dependent as the Horizon Report is on the voices of its panel, every effort was made to ensure those voices were diverse and that each could uniquely enrich the group's work.

This expert panel research utilized a modified Delphi process and elements adapted from the Institute for the Future (IFTF) foresight methodology. In the Delphi process, an organized group of experts discusses and converges on a set of forecasts for the future, on the basis of their own expertise and knowledge. For this report, panelists were tasked with responding to and discussing a series of open-ended prompts, as well as participating in subsequent rounds of consensus voting (see sidebar "Panel Questions"), all focused on identifying the trends, technologies, and practices that will be most important for shaping the future of cybersecurity and privacy in postsecondary education. Ideas for important trends, technologies, and practices emerged directly from the expert panelists and were voted on by the panel. EDUCAUSE staff provided group facilitation and technical support but had minimal influence on the content of the panel's inputs and discussions. This was done to protect the core intent of the Delphi process—capturing a reliable consensus from a group of experts that represents their collective expertise and knowledge.

The framing of the questions and voting across each round of panel input was adapted from IFTF's foresight methodology and drew upon the IFTF framework and process for collecting evidence and impacts for trends. Ensuring an expansive view across all the many factors influencing the future of higher education, the IFTF "STEEP" framework enabled our panel to focus on social, technological, economic, environmental, and political trends. This effectively broadened the panel's input and discussions beyond the walls of higher education to call attention more explicitly to the larger contexts driving cybersecurity and privacy practices. These larger trends—and the current evidence and anticipated impacts of these trends—served as the grounds on which the panel built its discussions on the emerging technologies and practices influencing postsecondary cybersecurity and privacy.

As they provided their inputs and engaged one another in discussion, panelists shared news articles, research, and other materials that would help reinforce their inputs and provide evidence for their particular viewpoints on current and future trends. In addition to enriching the panel's discussions and supporting the panel's voting and consensus processes, these materials were collected by EDUCAUSE staff for use as evidence and further reading in the writing of this report. In the Delphi and IFTF methodologies, these collected materials also serve the purpose of ensuring that the panel's future forecasts are sufficiently grounded in "real" data and trends.

For information about research standards, including for sponsored research, see the EDUCAUSE Research Policy.

Panel Questions

STEEP Trends

Round 1 (for each STEEP trend category):
In the appropriate STEEP category below, nominate trends that will impact the future of cybersecurity and privacy in higher education. Your nomination should include: (1) a sentence to describe the trend as the title of the card; (2) how this trend will impact cybersecurity and privacy in higher education; (3) links to supporting news or research; and (4) your name. Your name MUST be included to receive credit for the activity. To enrich the content, we encourage you to comment on the posts of your colleagues to add your thoughts.

Round 2 (for each STEEP trend category):
The list below summarizes the trends provided by this year's Horizon panel. Please rank order the trends based on which you believe will have the most/least influence on the future of cybersecurity and privacy in higher ed. Drag the six (6) trends from the left-hand list to the right-hand list and then rank them in the order of most influential (1) to least influential (6).

Round 3 (for each of the top 15 trends identified by the panel):

1. Please provide additional evidence supporting this trend. Make sure that your evidence is relevant to the future of cybersecurity and privacy in higher ed. Examples of good evidence include recent (i.e., within the last year) research reports, credible news stories, personal experiences, etc.
2. What potential impacts might this trend have on the future of cybersecurity and privacy in higher ed? Please be specific. Describe how this trend would impact not only cybersecurity and privacy in higher ed but also how resulting changes in cybersecurity and privacy would then affect stakeholders and different departments/units, academics, business operations, strategic planning and decision-making, etc.

Key Technologies and Practices

Round 1: For this round of information-gathering, we're interested in hearing from you about those key technologies and practices that you believe will have a significant impact on the future of cybersecurity and privacy in higher education.

What do we mean by "key technologies and practices"? For the purposes of the Horizon Report, these are practices that are either new or for which there is substantial, perhaps transformative, new development. An important dimension of these technologies and practices is that they have the potential to have significant impacts and effects on supporting cybersecurity and privacy. In particular, think about technologies and practices that have the potential to mitigate or accelerate the trends the panel has identified.

Your submissions should include a description of the key technology or practice, its impact on cybersecurity and privacy in higher education, and links to supporting news or research. Your name MUST be included to receive credit for the activity.

Round 2: The list below summarizes the key technologies and practices provided by this year's Horizon panel. From this list, please select the top twelve (12) items you believe will have the most influence on the future of cybersecurity and privacy. Drag those twelve (12) items from the left-hand list to the right-hand list and then rank them in the order of most influential (1) to least influential (12).

Round 3: Panelistswere asked to respond to the following questions about each of the top six technologies and practices:

- Why is <tech/practice> important for cybersecurity and privacy professionals?
- What specific action items related to <tech/practice> can you recommend for cybersecurity and privacy professionals?
- What risks, if any, might be introduced or exacerbated by <tech/practice>?
- How, if at all, does <tech/practice> impact diversity, equity, and inclusion?
- What further resources (e.g., news articles, institutional examples) about <tech/practice> can you suggest for readers of the Horizon Report?

EXPERT PANEL ROSTER

Jenay Robert
Senior Researcher
EDUCAUSE

Nicole Muscanell
Researcher
EDUCAUSE

Nichole Arbino
Senior Program Manager
EDUCAUSE

Mark McCormack
Senior Director of Research and Insights
EDUCAUSE

Jamie Reeves
Director of Community, Product, and Portfolio Management
EDUCAUSE

Ben Archer
Privacy Manager
Arizona State University

Jim Avery
Chief Information Officer
Union University

Joe Barnes
Chief Digital Risk Officer
University of Illinois System

Abe Bender
Senior Privacy Analyst
University of Washington

Ashish Bharadwaj
Chief Information Officer
Torrens University Australia

Karen Campbell
Chief Information Security Officer
Prairie View A&M University

Brad Christ
Chief Information Officer
Eastern Washington University

Wendy Epley
Principal Analyst, Information Security—Governance, Risk & Compliance
The University of Arizona

Joshua Fiske
Vice President for Information Technology
Clarkson University

Ricardo Fitipaldi
Chief Information Security Officer
San Diego State University

Joseph Gridley
Chief Data Privacy Officer
University of Maryland

Mike Hanson
Information Security Engineer
Ithaca College

Emily Harris
JD Candidate; Higher Education Cybersecurity Professional
Seton Hall School of Law

Allison Henry
Chief Information Security Officer
University of California, Berkeley

Bill Hunkapiller
Chief Information Security Officer
Florida State University

Greg Keane
Manager, Computing Ops
University of Delaware

LeeAnn LeClerc
Chief Information Security & Technology Officer
Worcester Polytechnic Institute

Nick Lewis
Program Manager, Security and Identity
Internet2

Venkata Malisetty
Data and Analytics Lead
California State University, Northridge

Rebecca Ortinez
Manager of IT Applications Development and Support
Noorda College of Osteopathic Medicine

Matt Parker
Director of Information Technology, SPIA
Princeton University

Pegah Parsi
Chief Privacy Officer
University of California San Diego

Lydia Payne-Johnson
Director, Data Governance, Compliance and Identity Management
The George Washington University

Jacob Picart
VP of Security Services
Apogee, A Boldyn Networks Company

John Ramsey
Chief Information Security Officer
National Student Clearinghouse

Jill Rasmussen
Critical Challenge Project Advisor
Brown University

Phil Reiter
Consultant

Chris Shull
CISO
Washington University in St. Louis

Stephen Streng
Research Development Strategist
University of Minnesota

Jerry Tylutki
Director of Information Security and Privacy
Hamilton College

Anthony Valentino
Lead Information Security Risk Analyst
University of California, Santa Barbara

Matt Williams
Chief Information Security & Technology Officer
The University of Tennessee

Ben Woelk
Governance, Awareness, and Training Manager
Rochester Institute of Technology

Scott Wood
Chief Information Officer
Baker College System