2021 EDUCAUSE Horizon Report®
Information Security Edition

EDUCAUSE

2021 EDUCAUSE Horizon Report®
Information Security Edition

Thank You to Our Information Security Horizon Report Sponsors

CISCO

FISCHER IDENTITY
DEFINING IDENTITY GOVERNANCE IN HIGHER EDUCATION

GreyCastle security

Microsoft

VANTAGE
Technology Consulting Group

Brian Kelly, Mark McCormack, Jamie Reeves, D. Christopher Brooks, and John O'Brien, with Michael Corn, Steve Faehl, Emily Harris, Keir Novik, Sherry Pesino, Peter Romness, and Greg Sawyer, *2021 EDUCAUSE Horizon Report, Information Security Edition* (Boulder, CO: EDUCAUSE, 2021).

© 2021 EDUCAUSE

This report is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

ISBN: 978-1-933046-07-5

EDUCAUSE Horizon Report is a registered trademark of EDUCAUSE.

Learn More

Read additional materials on the 2021 Horizon Project research hub, https://www.educause.edu/horizon-report-infosec-2021

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

Introduction

Since 2005, EDUCAUSE has helped to research and produce one of the longest-running considerations of trends, technologies, and practices shaping the future of higher education: the annual *Horizon Report*.[1] Using a methodology that grounds the findings in the perspectives and expertise of a panel of leaders in higher education, the report has helped those working with technologies in teaching and learning at colleges and universities around the world to better understand what lies ahead.

In 2021, EDUCAUSE is publishing a second edition of the *Horizon Report*. With this inaugural issue of the Information Security edition of the *Horizon Report*, we acknowledge that security and data privacy have an extraordinary and increasing significance on the horizon of higher education institutions. Ask any leaders at a college or university that has been the victim of a major security breach or that has succumbed to a ransomware attack, and they will make it very clear just how high the stakes have become.

Closely contemplating the horizon is critical during this unique time in our history. Even before the COVID-19 pandemic, privacy and security were topping the EDUCAUSE annual list of the top 10 IT issues in higher education. Because chaos and confusion always inspire (and help) bad actors to do their worst, we lately have seen an increase in menacing activity and continually more challenging risks to institutional security and privacy. With the dramatic shift to remote work and remote learning in 2020, threats are at an all-time high. The introduction of contact tracing, the increased use of home personal devices, and problems related to the proliferation of videoconferencing have ushered in unprecedented concerns.

Given the uncertainty, this report explores forecasts rather than predictions. As we've learned from the unpredictability of 2020, when we look to the future, we're more likely to see a set of possibilities rather than one obvious path forward. To delve further into those possibilities and forecasts, we asked the report panelists not simply to identify what might be impactful but to anticipate what that impact might be.

Those who have been longtime followers of the *Horizon Report*s focusing on teaching and learning will certainly see the value in a second edition. We trust that the information security community will gain an awareness and appreciation for the reports as well. The collective experience that was 2020 has taught us that teaching and learning issues and privacy and security concerns are fundamentally interconnected in the quest to advance higher education through the use of information technology. The EDUCAUSE QuickPoll surveys demonstrate that the pandemic has elevated the appreciation for technology as a strategic institutional asset. An October 2020 survey of senior IT leadership found that the operational and the strategic influences of information technology have increased since the beginning of the pandemic and that this influence is likely to continue post-pandemic.[2] As we look to the years ahead, technology innovation will continue to be a critical capability for colleges and universities. Securing these operations is not an optional priority but, rather, a crucial imperative.

—John O'Brien

1. *The Horizon Report* (Stanford: New Media Consortium and the National Learning Infrastructure Initiative, an EDUCAUSE Program, 2005).
2. D. Christopher Brooks, "EDUCAUSE QuickPoll Results: Senior IT Leadership," *EDUCAUSE Review*, October 9, 2020. All EDUCAUSE QuickPoll results can be found on the EDUCAUSE QuickPolls web page.

Executive Summary

With the 2021 Information Security *Horizon Report*, we have sought to expand our series of Teaching and Learning *Horizon Report*s to focus on a new area of critical importance to the future of higher education—the trends, technologies, and practices that are shaping the world of postsecondary information security. Based on a methodology that grounds the findings in the perspectives and expertise of a panel of leaders in higher education and information security, in this report we summarize the panel's input on the major trends shaping higher education, including panelists' reflections on the implications of this research for the future of higher education in their particular institutional contexts.

Trends

Higher education doesn't exist in a vacuum, and it is always and everywhere shaping and being shaped by larger macro trends unfolding in the world surrounding it. We asked the Horizon panelists to provide input on the macro trends they believe are going to shape the future of postsecondary information security and to provide observable evidence for those trends. To ensure an expansive view of trends outside the walls of higher education, panelists provided input across five trend categories: social, technological, economic, environmental, and political. After several rounds of voting, the panelists selected 15 trends as the most important. Unlike previous *Horizon Report*s, this list of trends includes one "uber trend" that was identified by the panel across multiple trend categories—remote work.

Social

- Information Security Workforce Shortage
- Greater Focus on Data Privacy
- Contract Compliance/Issues

Technological

- Borderless Networks / Network without Boundary
- Security Incidents Becoming Routine
- More Use of Personal Devices for Business

Economic

- Shift to Remote Learning
- Increased Collaboration in Higher Education and Research
- Mergers and Acquisitions in Higher Education

Environmental

- Data on Sustainability
- Increased Environmental Volatility
- Demand for Electricity

Political

- Authoritarian Surveillance
- Disinformation/Social Media Weaponization
- Deteriorating International Relations

Key Technologies and Practices

Horizon panelists were asked to describe those key technologies and practices they believe will have a significant impact on the future of postsecondary information security, with a focus on those that are new or for which there appear to be substantial new developments. After several rounds of voting, the following 6 items rose to the top of a list that initially consisted of 18 technologies and practices:

- Cloud Vendor Management
- Endpoint Detection and Response
- Multifactor Authentication/Single Sign-On
- Preserving Data Authenticity/Integrity
- Research Security
- Student Data Privacy and Governance

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 the institution. We asked panelists to consider those impacts along several dimensions that are of growing importance in higher education: equity and inclusion, positive impact on overall institutional information security, risks, end-user receptiveness, and cost. Panelists see considerable potential for all of these technologies and practices to have an impact on overall institutional information security, while student data privacy and governance was rated highest by the panel in providing needed support for equity and inclusion. Research security and endpoint detection and response were rated by panelists as the most costly techs and practices, and panelists reported an average level of receptiveness among end users across all six techs and practices.

Scenarios

While we may not be able to use the findings in this report to accurately predict a single future, we can begin to gather and arrange the information we have into logical patterns that can help us envision a number of scenarios for what the future might look like. In this report we attempt to paint brief but evocative portraits of four possible future scenarios for postsecondary information security:

- **Growth:** In ten years, cybersecurity professionals will be the linchpins of higher education, and cybersecurity staffing at institutions will have grown tenfold. End users will be informed and proactive partners in protecting their devices and networks, and there will be an increased focus on strategic and collaborative efforts across institutions to standardize approaches to cybersecurity.
- **Constraint:** Large mergers and acquisitions in the higher education ecosystem have left many IT budgets gutted, even as operating costs soar. Massive federal regulations on data privacy and protection leave higher education security professionals riddled with personal liability and under constant surveillance.
- **Collapse:** "Security fatigue" has taken hold across higher education and the developed world, and big tech giants are stepping into their role as the sole protectors of institutions' security. Institutions are making deep cuts or even eliminating internal cybersecurity functions, while student data is viewed as a commodity to profit from rather than an asset to protect.
- **Transformation:** The national movement toward remote work and online learning called for increased security and privacy efforts by institutions. To respond effectively, higher education partnered with national security agencies to mount a massive recruitment and training effort to proactively target cybercriminals and dismantle weaponized social media, disinformation campaigns, and propaganda factories in the "war on cyberterror."

Implications Essays

In light of the trends and future scenarios presented throughout this report, what can we say about the implications for institutions now and about what institutions can begin to do today to start preparing for these possible futures? For this section we asked seven Horizon panelists to reflect on the report's findings and offer their thoughts on the most important implications for their own higher education context.

The seven perspectives represented in these essays illustrate the ways in which issues overlap, diverge, and intersect in different parts of the world and at institutions of different sizes and types. Some contributors reflected on community mindfulness and responsibility when it comes to privacy and the potential for generational changes in privacy expectations, with more customers demanding information on how their data are used and stored. Other panelists took a deeper dive into the security and privacy implications of remote work and online learning, recognizing that the shifts we are experiencing will likely have staying power.

Though not intended to cover all perspectives, these essays can help catalyze thinking and conversations about the ways in which higher education is changing, the opportunities and risks it faces, and the ways in which technology and innovative thinking can help prepare institutions for the future.

Trends: Scanning the Horizon

For the inaugural 2021 Information Security *Horizon Report*, we begin by zooming out to capture a wider view of the world within which the practice of information security takes place. Recent global events—the COVID-19 pandemic, widespread adoption of virtual technologies, worsening environmental conditions, fraying international relations—have upended our lives both inside and outside our institutions of higher education and serve as the foundations for better understanding information security's present-day challenges and future opportunities. Acknowledging these trends, and better understanding where they may be headed, should serve as the beginning point for any discussion about our possible futures, and this is where we begin this report.

Recent global events have upended our lives and serve as the foundations for better understanding information security's present-day challenges and future opportunities.

To help us explore these larger forces taking shape around higher education, we asked our Horizon Expert Panel to survey the landscape around them and identify the most influential trends shaping higher education information security. To ensure that we identified a wide array of trends and not only those confined to the realm of higher education, we asked panelists to look across five broad categories: social, technological, economic, environmental, and political. This section summarizes the trends the panelists voted as most important in each of these categories, as well as the anticipated impacts of and examples of evidence for each trend.

As broad as the trends in this section are, they will certainly find many varied and more particular ways of being expressed through individual institutions and within local contexts. Though the voices of our Horizon Expert Panel captured in this section certainly do represent diverse perspectives from a range of institutions around the world, the issues covered in this section are far too complex to be fully nuanced over just a few short pages. We invite you, if you find important elements of your own context and story absent from these trend summaries, to share your experiences with us and the larger EDUCAUSE member community by emailing securitymatters@educause.edu or tagging EDUCAUSE on social media at @HEISCouncil and @EDUCAUSE.

Uber Trend: Remote Work

Social

Information Security Workforce Shortage

Greater Focus on Data Privacy

Contract Compliance/Issues

Technological

Borderless Networks / Network without Boundary

Security Incidents Becoming Routine

More Use of Personal Devices for Business

Economic

Shift to Remote Learning

Increased Collaboration in Higher Education and Research

Mergers and Acquisitions in Higher Education

Environmental

Data on Sustainability

Increased Environmental Volatility

Demand for Electricity

Political

Authoritarian Surveillance

Disinformation/Social Media Weaponization

Deteriorating International Relations

Uber Trend: Remote Work

More than any other single trend, the recent shifts in higher education to remote modes of working in response to the COVID-19 pandemic captured our panelists' attention and imagination through their discussions and voting. It is evident that the impacts of this "uber" trend on the future of higher ed information security are multifaceted and its evidence abundant. To try to fit remote work within only one of the five trend categories covered in this section would both seem to diminish the importance of this trend relative to the other trends and mischaracterize it as one type of trend and not any other.

The EDUCAUSE Horizon team made the decision, then, to designate remote work as an uber trend for this year's Information Security *Horizon Report*, pulling it out from the pack and signifying its singular importance to our panelists. Even with this special designation, the reader will likely see this trend continue to crop up through some of the other trends, as our remoteness and mobility in recent months has transformed many other aspects of our experiences of higher education. Indeed, if the trend of remote work persists, we believe it will have far-reaching implications for information security practice in higher education, its impacts felt globally and for many years to come.

Impacts: The impacts of remote modes of working and learning on the larger higher education industry seem almost incalculable. Optimistically, higher education leaders may now be in a position to explore innovative education practices and business models heretofore seen as impossible or too distant on the future horizon. Higher education may never be the same again after 2020, and that will be an exciting prospect to some. Others, however, will be less starry-eyed and may be dreading an inevitable financial collapse, fearing students will migrate away from remote experiences they view as less valuable than face-to-face experiences. Not all institutions will make the transition to a "new normal" successfully, some fear, and quite a few institutions may eventually be shuttered.

Whether one falls on the optimistic or pessimistic end of the spectrum or anywhere in between, it's hard to imagine a future for higher education that isn't dramatically different in some important ways. And those differences will be felt by information security professionals as much as, if not more than, anyone else at the institution.

The rise of remote work in higher education has the potential to reshape the very profession of information security itself. More open and flexible access to information security jobs might make it possible for institutions to attract a wider and more diverse pool of talent not constrained by geography. Moreover, information security units will be in the position of needing to fundamentally rethink how they do business, how they manage their staff and resources, and how they engage with partners and stakeholders across the institution.

Of course, the priorities of information security within a more remote higher education context will shift as well, and new roles and responsibilities for the profession will arise. Privacy concerns will be paramount as students, faculty, and staff do their work from personal spaces with their personal devices over personal networks. The traditional campus security perimeter will have vanished, raising urgent concerns around endpoint and cloud security and demanding new strategies around authentication and authorization. A remote future for higher education will redraw the lines around what and where protection is needed, and security professionals will have to reimagine the nature and scope of their work accordingly.

Evidence: Two Princeton graduates launch The U Experience, offering college students the opportunity to do their remote learning from luxury hotel "bubbles" in Arkansas and Hawaii, effectively "unbundling" the college experience from brick-and-mortar campuses. A global workforce survey from Dimensional Research finds that only 9% of workers expect to return to the office full-time in the future, while Slack's "Remote Employee Experience Index" finds that only 12% of skilled office workers intend to return to working exclusively from an office.

Social Trends

As the world around us changes and evolves, so too do our needs for more, better, and different approaches to information security. 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, those systems, and ourselves.

Information Security Workforce Shortage

Impacts: Our increasingly digital world will require a larger workforce of skilled information security professionals, and yet the supply of the information security workforce is expected to lag far behind the demand in the years ahead. Not only will institutions of higher education need to meet this increasing demand within their own expanded information security workforce but also will be looked upon to attract and educate the students who will eventually constitute that workforce, both inside and outside higher education.

Evidence: The US Bureau of Labor Statistics has estimated that the demand for "information security analysts" will grow 31% from 2019 to 2029, and yet the pool of talent for these jobs is falling well below what is needed. The University of West Florida has received a $6 million grant to address the information security workforce shortage by launching a new program for training military veterans and first responders for careers in information security.

Greater Focus on Data Privacy

Impacts: The proliferation of personal devices and individuals' near-constant connectedness through their online lives will continue to elevate the awareness and importance of individuals' data privacy, testing the boundaries of institutions' use and/or protection of personal data. More and more institutions will have to build up their privacy staffing and support, either through their existing information security units or through new, dedicated privacy units.

Evidence: The implementation of laws such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are requiring institutions to more carefully and systematically consider issues of personal data protection. EDUCAUSE's 2020 Student Technology study finds that only one in five students understands how their institution uses their personal data.

Contract Compliance/Issues

Impacts: The growing market power of big tech vendors will diminish individual institutions' agency and autonomy in negotiating customized contracts and security inclusions. Institutions strapped with standard vendor contracts will protect their interests through data-driven risk assessments. Legal risks in particular—compliance, risk of lawsuits—will drive much of institutions' assessments and decisions about vendors and solutions.

Evidence: A 2020 data breach that impacted numerous institutions and individuals illustrates the impacts caused by delayed breach notifications, which fail to comply with specific contract terms and requirements for many of those affected organizations. Due to increased higher education risks associated with factors such as the pandemic and increasing natural disasters, institutions are participating in purchasing consortia to negotiate insurance contracts and drive down premiums.

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 information security to keep pace with that ecosystem's ever-changing features and boundaries.

Borderless Networks / Network without Boundary

Impacts: Institutional services and data are becoming increasingly cloud-based rather than campus-based. Network endpoints (e.g., smartphones, laptops) are mobile and no longer confined to the campus, significantly expanding the boundaries of the digital world that must be monitored and protected. Institutions unable to isolate their own endpoints and network servers will experience diminished incident response control and increased incident response times.

Evidence: Verified Market Research estimates that cloud computing in the education sector will grow from a $15.3 billion market in 2019 to an $89.5 billion market by 2027. Stanford University launches its Cardinal Key program in an effort to strengthen protection and eliminate the need for passwords and authentications for web-based logins.

Security Incidents Becoming Routine

Impacts: Bad actors have developed more sophisticated and more professionalized strategies and attacks, and breaches and ransomware in higher education are on the rise. Incidents have become a part of institutions' normal business planning and operations, with institutions moving away from incident response and recovery to incident identification and prevention. A growing number of institutions have created "incident management" departments with dedicated incident leadership and support staff.

Evidence: According to a Redscan Freedom of Information (FOI) survey conducted in 2020, more than half (54%) of the UK universities in the survey reported a data breach at their institution over the previous 12 months. The UK's Open University is targeted by more than 1 million email attacks over the span of 9 months in 2020; all attacks are successfully blocked by the university's servers.

More Use of Personal Devices for Business

Impacts: With the proliferation of personal and mobile devices, along with institutions' continued adoption of virtual modes of working and learning, the use of personally owned devices (e.g., smartphones, laptops, tablets) for institutions' academic and administrative business has become more commonplace. Institutions are exposed to increased risks and challenges in keeping data and devices protected, leading to renegotiated boundaries around the institution's authority to monitor and control device and data use.

Evidence: Researcher and author Kenan Degirmenci has predicted that in 2021 the BYOD and enterprise mobility market will expand to $73.3 billion (up from $35.1 billion in 2016). EDUCAUSE's 2020 Student Technology study finds that an overwhelming majority of students are connecting two or more devices to campus Wi-Fi on a daily basis.

Economic Trends

Higher education faces enrollment and revenue challenges on the road ahead, and many institutions will have 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, information security in higher education.

Shift to Remote Learning

Impacts: As the higher education migration to remote modes of learning persists, institutions will continue to live under the threat of declining enrollments among students wary of online education, diminished institutional revenue, and tightened departmental budgets. The expanded security risks of remote operations and an increasingly mobile faculty, staff, and student body will demand more from information security units that are being asked to meet their institution's needs while working with limited staff and budget constraints on critical expenditures.

Evidence: An EDUCAUSE poll of IT leaders finds that 43% of respondents expect their IT budgets to continue to decrease into 2021, while a full 73% reported decreases in their institution's general fund reserves. The National Student Clearinghouse reports that undergraduate enrollments in the fall of 2020 were 4.4% below the previous year's enrollments.

Increased Collaboration in Higher Education and Research

Impacts: As institutional budgets become increasingly constrained globally, regional and consortial collaborations will be critical in helping institutions identify efficiencies and cost reductions in their information security needs. Institutions will leverage their collective buying power to drive down costs of information security solutions, and peer-based networks for information exchanges, shared decision-making, and industry-wide standardization will reduce effort in overcoming common information security challenges.

Evidence: The Council of Australasian University Directors of Information Technology (CAUDIT) launches its Australasian Higher Education Cybersecurity Service (AHECS) with the goals of aligning and coordinating information security practice across Australasian institutions and helping deliver economies of scale. Indiana University launches the NSF-funded Research Security Operations Center (ResearchSOC), intended to support the scientific computing cybersecurity needs of US institutions.

Mergers and Acquisitions in Higher Education

Impacts: Institutions already facing significant financial challenges will seize post–COVID-19 opportunities to merge with other institutions or to initiate shared or consolidated cross-institution services and operations while remaining independent institutions. Some information security units may find themselves stretched and shared across institutions, requiring considerable coordination and standardization as core information security functions become more centralized. Information security units navigating mergers or acquisitions will be called on to support the integration of knowledge assets and knowledge management systems, in addition to redesigning their institution's overall security business plans and strategies.

Evidence: The Pennsylvania State System of Higher Education (PASSHE) in 2020 announces plans to explore "integration options" for combining institutions across the state of Pennsylvania, in an effort to reduce costs in the face of declining student enrollments and state funding. The University of Arizona acquires Ashford University and announces its new University of Arizona Global Campus online education initiative.

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 landscapes in ways that necessitate new strategies for protection and security.

Data on Sustainability

Impacts: As climate change and other environmental issues transform our local and global communities, growing numbers of institutions of higher education will be required to provide extensive reporting and accounting of their sustainability efforts to funders and other oversight bodies. Data and privacy professionals will need to contend with new reporting standards and with balancing data transparency and data protection in meeting those new standards.

Evidence: The Sustainability Accounting Standards Board (SASB) and the Global Reporting Initiative announce a collaboration to develop standards in sustainability reporting to help both the organizations reporting their sustainability data and the bodies requesting/consuming those data. More than 300 colleges and universities have joined the Higher Education Sustainability Initiative (HESI), led by the United Nations Department of Economic and Social Affairs, with the goal of teaching and encouraging sustainability on campuses across the world.

Increased Environmental Volatility

Impacts: Extreme weather events (e.g., fires, hurricanes, floods) and dramatic shifts in climate patterns (e.g., record temperatures, droughts) drive technological innovations enabling institutions of higher education to adopt more sophisticated and networked tools for maintaining their facilities and monitoring campus safety. Expanded information networks and more connected tools will expose institutions to more and different security risks, requiring additional investments and support in information security.

Evidence: According to a CalMatters analysis, during the 2020 California wildfire season, 18 of California's 148 public higher education institutions were located in a fire hazard severity zone. Dozens of colleges and universities partner in 2020 to form the International Universities Climate Alliance, focused on sharing resources and encouraging research and innovation in response to climate change.

Demand for Electricity

Impacts: Institutions persist in their adoption of remote modes of working and learning, laying bare the dependence of higher education on reliable sources of electricity, as well as the uneven distribution of reliable electricity across local and global communities. Expanded energy production in underserved areas will lead to rising concerns over consumption and pollution, as well as enhanced security measures needed for protecting power grids from cyber attacks.

Evidence: As China returns to pre-COVID levels of activity and business-as-usual, so too do its levels of air pollution driven by contributing factors including coal-based power generation. In 2019, hackers successfully attack a power grid company in the western US, causing temporary disruptions and "blind spots" for power grid operators.

Political Trends

National and global political movements vie for influence and power, and they exploit technologies and social media to seize that influence and power. Rising nationalism and international tensions lead to dramatic shifts in the rules of engagement and cooperation between nations. Against this volatile political backdrop, information security professionals remain vigilant, exploring new strategies and partnerships for preserving truth and safety.

Authoritarian Surveillance

Impacts: While many governments continue to move in the direction of imposing sweeping privacy regulations (e.g., GDPR), others remain more laissez-faire and fragmented in their approaches to controlling and safeguarding data. The lack of consistent privacy laws and regulations across state and national borders leads to widespread and frequent compliance challenges. Institutions of higher education in the United States encounter significant barriers to international collaborations due to complex and often unsolvable differences in data policies and practices.

Evidence: US National Institutes of Health (NIH) adviser Robert Eiss reports that GDPR restrictions have stalled at least 40 medical studies on cancer risk factors and exposures. China announces its new Personal Information Protection Law, imposing restrictions on the collection and use of personal data.

Disinformation/Social Media Weaponization

Impacts: The use of deepfake videos, believable disinformation, and weaponized social media becomes more commonplace on the global social and political stages, and governments and institutions of higher education lag behind in their capabilities for understanding and preparing for the security implications of these activities. Security professionals explore innovative solutions and develop new partnerships with social media and technology industry leaders, political scientists, and policy makers.

Evidence: The journal *Nature* publishes research findings detailing the successful spread of false COVID-19 "anti-vax" messages and conspiracies through social media. Researchers at Stanford University and UC Berkeley unveil new AI-based technology for detecting deepfake videos.

Deteriorating International Relations

Impacts: Divisions and tensions continue to grow globally between leading nations, with relations between the United States, China, Russia, Iran, and North Korea deteriorating and lurching forward in unpredictable and potentially dangerous directions. Higher education leaders will be tested as they navigate new policies and norms around international partnerships and influence in their practices and policies, and information security units will be called on to improve and expand their monitoring and protection measures against bad actors.

Evidence: Harvard University's Charles Lieber is arrested for failing to disclose his participation in China's Thousand Talents Plan, a Chinese recruitment effort designed to attract scientific talent for the furtherance of China's national interests. The US Department of Education launches an investigation into universities' underreporting of gifts and contracts received from foreign governments.

Key Technologies & Practices

Given the major trends taking shape outside and inside higher education, information security professionals and their institutions may need to begin planning now for specific technology solutions and practices—or even deploying them—to be better positioned for success in the future. Importantly, these technologies and practices have the potential not only to be mere reactive solutions for what is already taking place in higher education but also themselves may have the potential to actively change the future landscape of higher education in profound and lasting ways.

For this report, the Horizon panelists began with a blank slate and were tasked with identifying the technologies and practices they believed would have a significant impact on the future of higher education information security. Through several rounds of panelist voting, an initial roster of 18 candidates was reduced down to the list of 6 key technologies and practices presented here.

Cloud Vendor Managment

Endpoint Detection and Response

Multifactor Authentication/ Single Sign-On

Preserving Data Authenticity/ Integrity

Research Security

Student Data Privacy and Governance

- Cloud Vendor Management
- Endpoint Detection and Response
- Multifactor Authentication (MFA)/Single Sign-On (SSO)
- Preserving Data Authenticity/Integrity
- Research Security
- Student Data Privacy and Governance

The inclusion of practices in this section, beyond merely focusing on technologies, is important to highlight and situate within the longer history of higher education *Horizon Report*s. In previous Teaching and Learning editions of the report, many of the important developments in higher education were clearly not based solely on technologies. Examples include MOOCs (2013), flipped classrooms (2014 and 2015), mobile learning (2017 and 2019), makerspaces (2015 and 2016), and the elevation of instructional design, learning engineering, and UX design (2020). Certainly all of these rely on technology to enable the practice, but each is more a practice than a technology. Similarly, in the expert panel discussions for this report, enlarging the panel's focus to include practices has made it possible to bring into relief a more accurate picture of what is influencing postsecondary information security.

What kinds of challenges might institutions encounter if they go forward with any of the technologies or practices identified by the expert panel? And what kinds of benefits might they expect? To assess the nature and extent of the impact of these key technologies and practices, we asked panelists to evaluate each of them across several dimensions, using a five-point scale (0 = none; 4 = highest):

- How useful will it be in addressing issues of equity and inclusion?
- What is its potential to have a significant and positive impact on overall institutional information security?
- What is its risk of failure?
- How receptive will end users (e.g., faculty, staff, students) be to adopting it?
- What level of institutional spending will be required to adopt it?

In this way, we asked the panelists not simply to identify what might be impactful but to anticipate just what that impact might be. These results are presented in the charts that accompany the discussions of the technologies and practices.

Cloud Vendor Management

Vendor management has long been a feature of higher education IT operations, as institutions strive to balance the systems and solutions that they have the capabilities for managing in-house and those systems and solutions requiring third-party support and/or expertise. The integration of vendor products and services into the institution's ecosystem raises perennial challenges and questions around the "fit" of that vendor with the institution's culture, values, budget, and needs, and these integrations impress upon IT leaders the need to continually and thoughtfully manage the relationship of the vendor with the institution.

Successful vendor–institution relationships rely on the alignment of shared goals, frequent and clear communication between key stakeholders, and collaborative approaches to support, problem solving, and service improvement. Cloud services in particular are becoming increasingly important to institutions as an efficient solution for their IT needs, and the effective management of the relationships with cloud vendors will be at the crux of institutions' successes or failures in more remote and virtual environments on the road ahead.

Overview

Opportunities for shifting operations and services to the cloud have for years now captured the attention and even enthusiasm of IT leaders eager to find more efficient and cost-effective approaches to supporting their institution. And for as long as it has captured our attention and enthusiasm, this approach has also stirred our concerns over the safety of the systems and assets we migrate to the cloud. Though some might argue that cloud-based solutions offer even more security than in-house solutions, the cloud has nonetheless presented IT and cybersecurity professionals with new questions about the risks and security measures that will be required of us to protect the institution.

Over the past year, institutions have accelerated the move of many of their operational needs and services online in response to the COVID-19 pandemic. As these institutions explore possibilities for maintaining remote modes of working and teaching and learning in a post-pandemic world, cloud-based solutions stand to become even more critical for operations than they are now and will come to support more and more the educational and research aspects of the institution's operations and services.

For many institutions, third-party, vendored approaches to adopting needed cloud capabilities will be the preferred path to securing solutions more efficiently, less expensively, at scale, and with the benefit of vendors' resources, support, and expertise. Many institutions lack the internal resources, staffing, and/or expertise for standing up cloud-based solutions in-house, as well as for protecting those solutions, and are simply not at a level of capability that matches that of the larger cloud service providers.

With this increasing reliance on third-party cloud service providers, institutions' focus will be shifting away from managing the services themselves and more toward managing their relationships with the vendors who provide those services. Successful implementation of cloud solutions therefore has become more dependent on vendor vetting and selection, contract negotiation and procurement, ongoing assessment of the relationship and services, and evaluation of the safety, incident response actions, and needs of those solutions.

Cloud Vendor Management in Practice

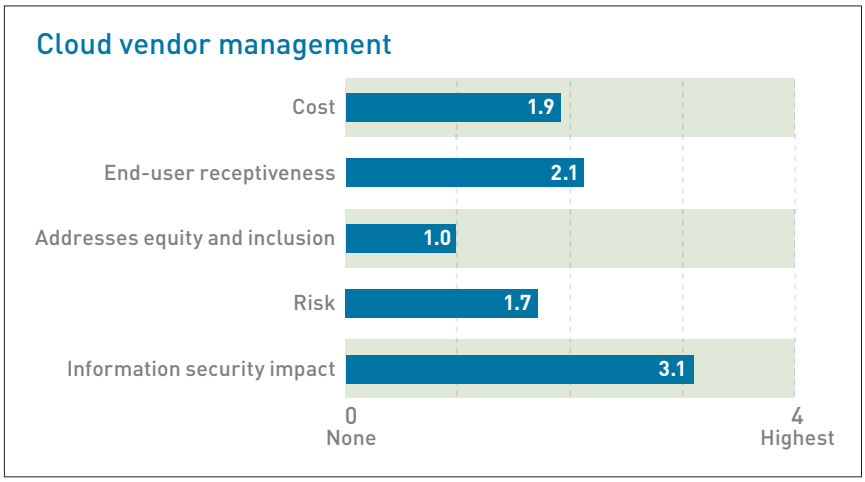
University of California, Berkeley: Using HECVAT for High-Risk Vendor Assessments

EDUCAUSE's Higher Education Community Vendor Assessment Toolkit (HECVAT) is an essential part of the campus vendor assessment process for high-risk supplier contracts. UC Berkeley leadership reviews HECVAT responses in conjunction with a supplier security plan and supplemental documentation (e.g., SOC report, PCI DSS AOC) to assess compliance with policy and relevant regulatory data security and privacy requirements (e.g., FERPA, GDPR, HIPAA). The end result is an assessment report with a "Recommend" or "Not Recommend" overall rating, along with recommendations for any mitigations.

Michigan State University: IT Readiness + Service Provider Security Assessment

At Michigan State University (MSU), the Service Provider Security Assessment (SPSA) process is the key to assessing where risk lies before accounts are reconciled or before a technology purchase has been completed. MSU IT has partnered with the MSU Purchasing Department and the Office of General Counsel to develop a robust set of questions to screen for the "IT Readiness" of a product, which then allows for further decisions on whether a risk assessment (HECVAT) is warranted.

Relevance for Information Security



Cloud vendor management introduces a number of important implications for cybersecurity in higher education, as illustrated in the figure. The overall impact of this practice on the institution's cybersecurity posture (3.1), as rated by our panel of cybersecurity experts, is notably higher relative to its perceived cost and risk. Lower cost, of course, may be one of several primary motivating factors for institutions exploring a vendored solution in this area. And the vendor's robust resources, staffing, and expertise, as well as the relatively hands-off nature of the institution's involvement in these services when managed by an outside vendor, may contribute to feelings that these vendored solutions are a relatively low-risk proposition for the institution.

That none of the techs and practices identified by our expert panel scored all that highly in either "end-user receptiveness" and "addresses equity and inclusion" is curious and may relate to a perceived disconnect between the work of cybersecurity professionals and the immediate experiences of the end user. One might view the work of cybersecurity as taking place "behind the scenes" and as functioning successfully when its presence isn't felt or observed by the end user. It's unlikely that a student or faculty member would know or care much about the management of a cloud vendor relationship, so long as it's done effectively and in a way that doesn't disrupt the work of being students and faculty or disrupt the resource and service access that the vendored solution provides.

Further Reading

EDUCAUSE
Higher Education Community Vendor Assessment Toolkit (HECVAT)

EDUCAUSE Review
Tying Up Loose Ends in Transitioning to the Cloud

EDUCAUSE Review
Rowing Together, Vendors and CIOs Navigate Tricky Relationships

Endpoint Detection and Response

Desktop computers. Laptops. Smartphones. Tablets. These and other devices serve as the gateways through which students, faculty, and staff engage with their institution and carry out their work in higher education. They also serve as one of the primary gateways through which institutions are exposed to cyber risk and the threat of breaches and other incidents detrimental to the institution's safety. As these devices increase in number and extend their reach into our day-to-day living and across our campuses, cybersecurity professionals' efforts to protect these devices and monitor their activities will become even more paramount to institutions' overall security posture well into the future.

Overview

According to Absolute's *2019 Endpoint Security Trends Report*, 70% of all security breaches originate at endpoint devices through vulnerabilities such as compromised credentials or a degraded security system. Recent years have seen a proliferation of endpoint devices owned and operated by the average person, and the typical device has 10 or more endpoint security agents installed. Given the complexities and challenges of testing and monitoring endpoint security and of resolving any needs or issues that can arise at each endpoint, endpoint security just might be institutions' most urgent and vexing source of cyber risk and threat.

The web of connected endpoints that support our daily lives—personal, professional, and educational—is expanding. On average, students on campus are connecting two or more devices (e.g., smartphones, laptops, tablets) to campus Wi-Fi on a daily basis. Meanwhile, our homes are more connected now than ever, with our dishwashers and vacuums and televisions and other "things" all wired to the internet and with the number of Internet of Things (IoT) devices expected to increase to 43 billion by 2023 (a threefold increase over 2018).

End users' concerns over safety and their willingness to follow best safety practices in their uses of this complex web of devices and networks are critical ingredients for institutional success in endpoint security. While it is encouraging that most students and faculty at least pay lip service to the importance of security while using their devices and accessing networks, the convenience of easy and seamless access is still a feature many of them have come to expect, and these expectations may in practice contribute to diminished awareness or shortcuts in safety and opportunities for heightened risk to the institution.

These challenges have been further compounded by the 2020 migration of most higher ed staff, faculty, and students to remote modes of working from home, parking lots, and other off-campus locations. More and more end users have been and will continue to use their own personal devices to work from their own personal spaces, using their own personal networks. Cloud-based endpoint protection platform (EPP) solutions will become far more desirable and essential for managing the institution's security, enabling remote monitoring of network and device activity, and conducting remote remediation when endpoint incidents occur.

Endpoint Detection and Response in Practice

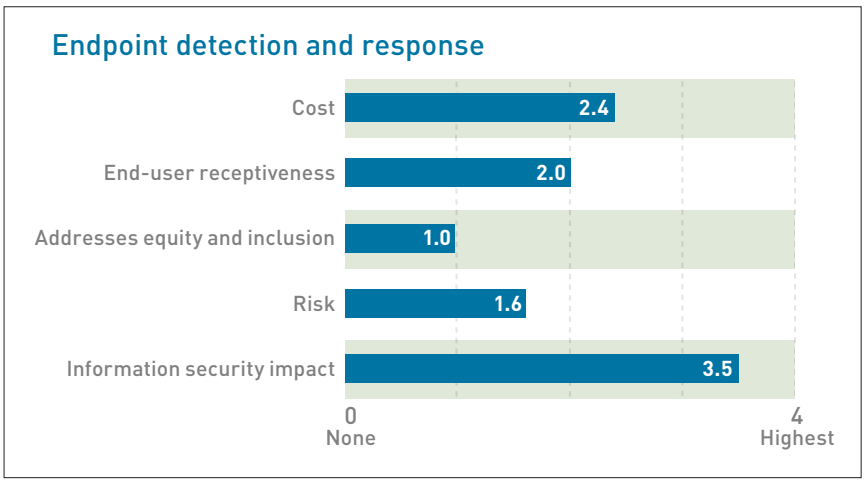
Bloomsburg University of Pennsylvania: Crowdstrike Falcon

Over the past few years, Bloomsburg has piloted the development of Crowdstrike Falcon, a new security agent that supplements the work of the institution's standard endpoint protection system. When endpoint protection flags a machine for investigation, Crowdstrike Falcon is loaded to provide more detailed information, including what the threat is, where in the chain it was stopped, and data on what it was and where it came from. This information can be used to formulate future configuration changes and protections on university endpoints.

University of Richmond: Endpoint Protection Replacement

University of Richmond's Information Services Division launched an effort to evaluate, select, and implement a new EPP that would detect malware and malicious behavior on an endpoint to prevent further compromise of a computer or network. This project included the selection of an EPP that would provide endpoint detection and response capabilities along with next-generation antivirus prevention for managed computers. Since the implementation of this new system, information services staff have seen fewer infected computers and are able to respond to threats before they have an adverse effect in the environment.

Relevance for Information Security



Of the techs and practices identified by our panel of cybersecurity experts, endpoint detection and response received the second-highest rating of "impact" on information security at the institution. This outcome makes sense when one envisions a future characterized by an increasingly complex web of devices, both personal and professional, that put the institution at risk and demand the cybersecurity professional's dogged attention and support. It also reinforces the finding noted above that the vast majority of all security breaches occur through the gateway of the endpoint.

The "balanced" score (2.0) of end-user receptiveness perhaps squares with what we know to be the end user's views of security and convenience in using their devices and accessing their networks, and this midpoint finding may be of more concern here than with other technologies and practices in this report, given the critical role of the end user in endpoint security.

Endpoint detection and response also received the second-highest rating in the category of cost. Mirroring the other techs and practices summarized in this report, endpoint detection and response received a low rating in the category of equity and inclusion, as well in the category of risk. Indeed, if there is a risk to the institution related to endpoint detection and response, it is in not deploying a solution in this area and in failing to shore up the institution's protection against one of its greatest vulnerabilities.

Further Reading

EDUCAUSE

2020 Student Technology Report: Supporting the Whole Student

EDUCAUSE Review

Risk Management Through Security Planning: Lessons from a CIO and CISO

Multifactor Authentication/Single Sign-On

As the number of applications and systems that faculty, staff, and students need to access on a daily basis increases, the demand and expectation for solutions that protect accounts while simplifying the authentication process are expected to increase as well. Having seamless and easy-to-use multifactor authentication (MFA) and/or single sign-on (SSO) options might not be a campus differentiator today, but it may very well be in the near future. Although the task of implementing such tools is a difficult one for many higher education institutions, given the complexity of the IT systems at a typical college or university, we need to find ways to simplify access to those systems so that end users can have the most secure and convenient authentication process available to them. If MFA and SSO can live up to their promise, gone will be the days of maintaining handwritten lists of usernames and passwords in a drawer, on the back of the device, or in password lockers.

Overview

Multifactor authentication is a digital authentication method by which individuals are granted access to applications and/or platforms after presenting two or more pieces of evidence to verify their identity. Factors are typically drawn from two or more of the following types of information: (1) something you know (e.g., password, username, PIN, answers to security questions); (2) something you have (e.g., token, smartcard, smartphone); (3) something you are (e.g., biometrics such as a fingerprint, retina scan, voice recognition); or (4) somewhere you are (e.g., location data). MFA is effective precisely because bad actors typically do not have access to more than one of the factors; account owners are typically alerted to attempted hacks by requests to authenticate through the other factors.

Single sign-on provides users with the ability to authenticate one time for automatic and subsequent access to various applications and platforms within and/or across systems. By eliminating the need for separate logins that require unique usernames and passwords, SSO makes navigating systems easier for the end user. It reduces the probability of lost, forgotten, or stolen credentials resulting in breaches of security. When combined with MFA, SSO can be a powerful tool to protect valuable institutional data.

The products and services that constitute authentication technologies for MFA and SSO are numerous, and the combinations of systems and approaches deployed vary by institution. Although institutions tend to focus their MFA and SSO efforts initially on those staff and faculty whose access to sensitive information and systems requires the highest degree of security, the subsequent ease with which these technologies are scaled to the entire campus and rendered user-friendly is noteworthy. For example, Stony Brook University took the approach of enrolling individuals and services into its MFA solution. This approach instantly enhanced security for individuals who were already enrolled, and it also provided a simple alternative to expedite the enrollment of additional services into MFA. Duke University created Duke Unlock, a one-step, password-less MFA solution integrated with Duke's Shibboleth environment.

MFA/SSO in Practice

No Phishing

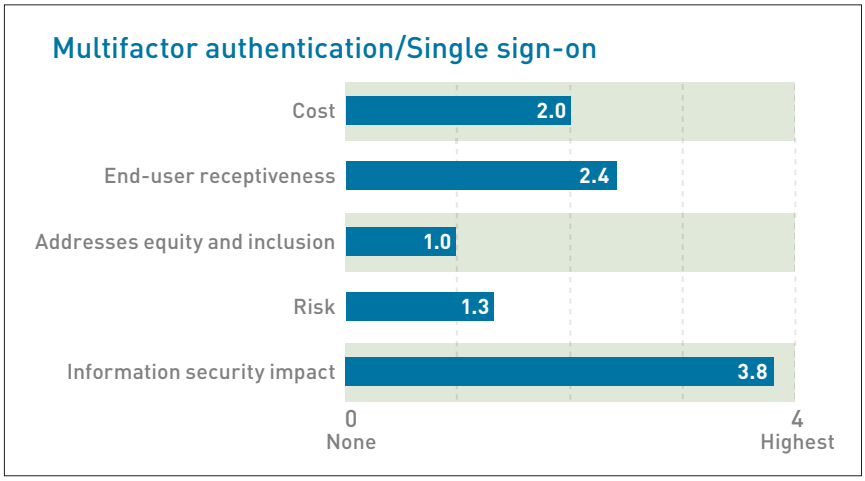
Vassar College greatly enhanced and improved its overall information security profile through investing time and resources into a comprehensive effort to re-architect its identity and access management systems, including new updated password rules, an SSO platform, and Duo MFA. The project has reduced phishing in that the standard login screen for Vassar's applications is the same, preventing users from falling for schemes that model other login pages.

MFA/SSO for All

Simon Fraser University used an existing institutional SSO layer to deploy a reliable, on-premise, MFA system that supports not only web applications but also services such as data center and VPN access. Initially targeting only high-profile/high-risk users in central systems, Simon Fraser supported a mandate to make MFA required for all accounts at the institution and to adopt a central SSO system to protect the identities of 30,000+ users, a feat that would have otherwise been cost prohibitive from a licensing standpoint.

This solution opens the door to enhanced security and convenience by allowing users with Duke network credentials to skip using their password and second verification step when logging in from a registered personal device. Bloomsburg University of Pennsylvania expanded its MFA program to include students who have part-time jobs in various offices around campus to give them VPN access to be able to continue to work remotely during the pandemic. Simon Fraser University issued an MFA mandate for all accounts at the institution and adopted a central SSO system for all faculty, staff, and students.

Relevance for Information Security



Of the six key technologies and practices featured in this *Horizon Report*, MFA/SSO is the one expected by our Horizon panel experts to have the greatest impact on higher education information security (3.8), while posing the lowest overall risk (1.3). Panelists believe it can be implemented at a moderate cost (2.0). And, although MFA/SSO is not expected to address issues of equity and inclusion very well, end users are expected to be rather receptive to using them in order to protect their accounts.

Adoption of MFA and SSO authentication solutions may lay the foundations for the realization of truly adaptive authentication technologies. Adaptive authentication determines the number and type of authentication factors required to access platforms and applications based on end users' locations, roles, and permissions. For example, someone logging into the ERP from an institutionally provided device while on campus using a secure network presents a low risk, requiring only a minimum level of authentication. That same person accessing the ERP from an unsecured hotel kiosk in southeast Asia on a personal device might be required to provide every available security factor.

Further Reading

EDUCAUSE Review

A Case for Open-Source Multifactor Authentication Security in Higher Education

University Business

Multifactor Authentication Strengthens Cybersecurity across University Campus

Secplicity

Security in Higher Ed: Trust, Student Experience, and Multi-Factor Authentication

Preserving Data Authenticity/Integrity

An accidental deletion or misplacement of a byte of data can change its validity, leading to drastic consequences in medical research; imagine the impact of falsified or manipulated research data on the development of a critical vaccine or the side effects of a new medication. Maliciously falsified or manipulated data can ruin a career or a promising line of research. The relative ease with which "fake news," doctored images, and deepfake videos can be created and distributed to promote disinformation and conspiracy theories makes it increasingly difficult to identify, debunk, and remove those bogus artifacts. The more that data are open and available, the more likely bad actors will seek to undermine our confidence in data. The role of information security professionals in protecting data from internal and external threats is growing, and the implications for not preserving data authenticity and integrity in higher education are increasingly dire.

Overview

Data authenticity depends on the ability to prove that data are not corrupted after their creation. Strictly speaking, the authenticity of any data that have been processed or prepared for delivery to end users can be said to have been compromised. In the real world, raw data needs to be cleaned (and, in this way, corrupted, in a technical sense) in order to render those data usable without compromising what the data actually represent. In the simplest terms, data authenticity exists when the data are what they are supposed to be.

Data integrity is represented by the often overlooked "I" in the CIA triad of confidentiality, integrity, and availability. Data integrity can be maintained even when strict data authenticity is violated, as described above, provided that those who are modifying or deleting data are authorized to do so. For example, the correction of errors and/or updates to data performed by individuals or systems sanctioned to do so preserves the integrity of the data, even while potentially diminishing data authenticity. Many of the threats to data integrity are the products of human agency, whether unintentional or malicious. Here it becomes critical to maintain file permissions, access controls, and version control and to establish/record rules by which data are altered or deleted. Additional threats to data integrity result from events such as server crashes, electromagnetic pulses (EMPs), or natural disasters; such threats might be avoided or mitigated by backups and/or redundancies.

Efforts to preserve data authenticity and integrity are inextricably bound up with network and endpoint protection, as well as general applications of protocols and standards for the protection of credentials, devices, and data. Future efforts will require information security teams to pay more specific attention to the data themselves and to allocate greater effort and more resources to techniques for verifying authenticity. These efforts can include risk-based validation of data, business continuity plans, verification of system inputs, careful selection of systems and service providers, and regular archiving of data.

One of the more challenging aspects of preserving data authenticity and integrity is guarding against human behavior. As malicious entities become increasingly sophisticated in their methods of surreptitiously gaining access to data, higher education institutions would be well served to train end users to think critically about how they might be the sources of potential violations of the authenticity and integrity of data to which they have access. To combat the threats to data via the end user, institutions such as Stony Brook University are reimagining

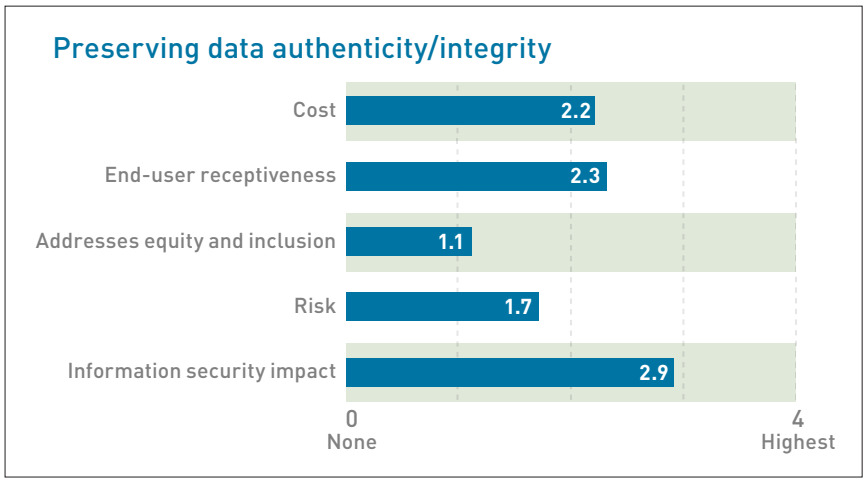
Preserving Data Authenticity/ Integrity in Practice

Internal Phishing Challenge

Stony Brook University modified its traditional security awareness program to include a gamified phishing exercise that challenged end users to recognize a series of increasingly sophisticated fake phishing attempts, initiated by the institution. Those who were duped and clicked on the links were provided information about how they were tricked and directed to a training module to help them identify phishing attempts; those who did not click were rewarded with a congratulatory note and commendation.

their security awareness efforts to include a training module to identify phishing attempts, followed by a series of phishing attacks that are announced and choreographed by the IT department. Those who click on the links to the earlier and easier ones are reassigned to the training module; those who are tricked later are taught how they could have identified the message as a phish and are encouraged to revisit the original module; those who don't fall for the phishing attempt receive a congratulatory message. The impact of the training exercise has been judged to rival some of the technical controls in place to preserve data authenticity and integrity.

Relevance for Information Security



The Horizon Expert Panel thinks that preserving data authenticity and integrity will have a significant impact on higher education information security (2.9). End users are expected to be more receptive than not (2.3) to preserving data authenticity and integrity, but the costs may be a bit higher than for other technologies and practices (2.2). While risks associated with data authenticity and integrity preservation efforts are moderately low (1.7), the impact on issues related to equity and inclusion is expected to be minimal.

While cost may be the biggest downside to securing the human and technological resources required to build, deploy, and maintain the systems needed to preserve data authenticity and integrity, the greatest limitations on the effectiveness of such endeavors may very well be the susceptibility of the end user to the deceptive tactics of those seeking to exploit data vulnerabilities. Technical and procedural approaches to shoring up data authenticity and integrity, such as file permissions, access and version controls, codebooks and dictionaries, endpoint detection, and credential and device maintenance, can only do so much. Providing comprehensive and periodic training, especially for those with access to sensitive data, to identify, avoid, and report phishing scams and other threats is a necessary step but, by itself, is insufficient to keep Dave from being the vector whose compromised credentials lead to the alteration and/or deletion of institutional data.

Further Reading

EDUCAUSE Review
A Data and IT Governance Journey: Finding Truth Amid the Quicksand

Clemson University Media Forensics Hub
Spot the Troll

National Cybersecurity Center of Excellence
National Cybersecurity Center of Excellence: Data Security

Research Security

One of the foundational purposes for which institutions of higher education exist is to produce and share knowledge, not only through instruction in the classroom but also through the explorations and discoveries of research. As institutions' modern research practices have become dependent on computing and digital technologies, this longstanding pillar of the higher education institution has also become one of its primary sources of cybersecurity risk. Research data, oftentimes highly sensitive in nature, have become digital assets that institutions now must work to protect from foreign and domestic actors, and the devices and systems that produce and store those data must be guarded as remote gateways for breaches into the institution.

Overview

Academic research has long been considered a hallmark of higher education, one that may increase in value for institutions as higher education models evolve and institutions carve out a niche in society in the future. Built on the values of open inquiry, creativity and innovation, and freedom of expression, the practice of research may at times seem at odds with other institutional values of monitoring and safeguarding institutional assets. Indeed, finding an appropriate balance between these seemingly competing values and priorities will be a necessary challenge for institutions seeking to simultaneously preserve the institution's commitments to creating and sharing knowledge and its need to be protected from real and ever present threats.

Since World War II, federal and industry support for research at US colleges and universities has steadily increased, today serving as a sizable source of funding for academic researchers through centers such as the National Institutes of Health (NIH), the National Science Foundation (NSF), and the Department of Defense. While these investments in research have undoubtedly led to significant scientific, medical, and other global advancements, some of these entanglements within universities have not been without controversy and criticism. At a minimum, they've raised questions around objectivity and the freedom of inquiry. At worst, they've exposed universities and researchers to interference and influence from those seeking to leverage institutional resources for their own (sometimes nefarious) purposes.

Institutions have explored and will need to continue building strategies for mitigating risks to research security and ensuring that institutions and their data are protected from potential threats. For research tied to federal and industry funds and partners, the US Office of the Under Secretary of Defense for Acquisition and Sustainment has developed a Cybersecurity Maturity Model Certification (CMMC) framework intended to ensure appropriate security practices for protecting federal contract information (FCI) and controlled unclassified information (CUI). Beyond federal and industrial initiatives, collectives of institutions have worked together to identify solutions for research security more broadly, as with the collaboration between the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU) in surveying and cataloguing institutions' successes and promising practices in ensuring their research security.

Research Security in Practice

OmniSOC

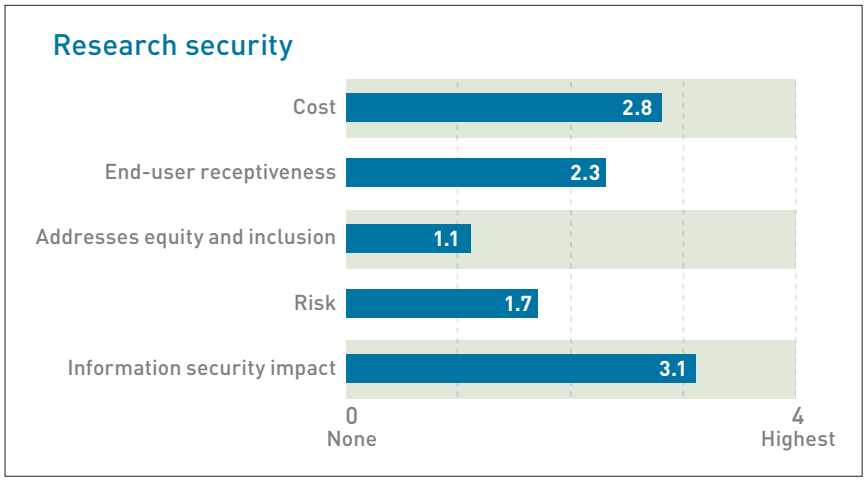
Founded by Northwestern University, Purdue University, Rutgers University, the University of Nebraska–Lincoln, and Indiana University, OmniSOC is a shared cybersecurity operations center that collects cybersecurity data from partners, integrates those data with other threat intelligence, and monitors, triages, and analyzes security events. Located at IU, OmniSOC also supports the ResearchSOC, the NSF Security Operations Center, and is a proud member of the Indiana University Cybersecurity Community.

Kansas State University: Research Information Security Enclave

The Research Information Security Enclave, or RISE, was developed by Kansas State University, in partnership with Microsoft, in response to requirements from the federal government for safeguarding controlled unclassified information (CUI).

Individual institutions themselves have also explored strategies for improving their own research security posture. MIT has implemented a new review process for research projects considered to be an "elevated risk" for the institution, such as projects funded by individuals or entities associated with known threat. And Penn State has collected a suite of resources for researchers in navigating international research collaborations, including information on institutional and federal policies and best practices for researchers.

Relevance for Information Security



Of the six technologies and practices identified by our panel of cybersecurity experts, research security received the highest score in the category of cost. With this score, research security also has the smallest gap between perceived cost and perceived impact on the institution's information security. This more equal balance between cost and impact could conceivably lead to difficult decisions at the institution in weighing potential investments in research security against the benefit of those investments to the institution, resulting in compromises or shortcuts in shoring up that area of security for the institution. While federal- and industry-funded research may demand security measures as a matter of compliance and not of choice, other areas of research may see their investments in security neglected or under-resourced.

Managing the trade-offs between convenience and security is a perennial challenge for cybersecurity professionals working with end users to ensure safer practices. End-user receptiveness to research security likely will depend on these same trade-offs and may also be dependent on the type of research the end user is engaged in and on their sources of funding and support. Faculty and researchers not accustomed to heightened attention to research and data security, and those not trained or experienced in the use of security-related solutions, may resist adopting new tools or practices in the course of doing their work. Researchers more accustomed to security practices, on the other hand—e.g., those with experience working on federal contracts—may be more willing and experienced partners in ensuring the safety of their data and practices at the institution.

Further Reading

EDUCAUSE
Networking to Support Data-Intensive Research: A View from the Campus

EDUCAUSE Review
EDUCAUSE QuickPoll Results: Academic Research

EDUCAUSE Review
Give Me Security, Give Me Convenience, or Give Me Both!

Student Data Privacy and Governance

Today's students are generally perceived to be savvy and sophisticated in their understanding of data privacy. They ask the right questions. They are aware of the potential risks in letting higher education institutions use their personal data. And they are opting out more than ever before. They are discerning about the type of data they allow their institutions to collect and use. At the same time, they know very little about how their institutions use their data and are uncertain about the benefits conferred by the use of their data. And while students trust their institutions to use their data appropriately, the lack of transparency around what is collected, how it is used, and how it benefits students undermines both trust and confidence in the institution to protect their data. Students increasingly expect higher education institutions to protect their data, to use their data responsibly, and to allow them opt out of personal data collection and use. For this to happen, institutions need to implement robust data governance regimes with clear privacy protections and adopt privacy management tools for student use.

Overview

Colleges and universities collect a lot of data on their students. Data collection begins as soon as students apply for admission or—in cases where students send institutions their test scores directly—before applications are even submitted. Data collection continues throughout the entirety of students' academic careers and includes everything from LMS use to rec center visits, cafeteria selections, library resources used, and building access. And, to the extent that they have contact information for graduates, institutions gather data on alumni.

At issue is whether institutions should be collecting all of this information on their students. If not, which data should be collected, who should get to use the data, and for what purposes? Collectively, the rules that specify the decision rules and accountability for proper behaviors associated with the collection, use, storage, protection, and destruction of data are known as data governance. Every institution needs to develop and promulgate a robust data governance regime that directly addresses issues related to the protection and management of students' personal information.

As students become more aware of what information institutions are collecting on them and how it is being used, they will want to exert more control and agency over their data. Privacy management tools can facilitate institutional audits of compliance with privacy regulations, track incidents that jeopardize sensitive personal data, track which data are collected and how they are used, and document user awareness of privacy policies. More mature privacy management tools would feature public-facing dashboards and allow end users to manually determine which data institutions are allowed to collect and use.

Student Data Privacy and Governance in Practice

The Maryland Public Higher Education Privacy Law

The University System of Maryland worked with the Maryland legislative and executive branches to draft a privacy law to protect the personal information of its community members, give its community members greater access to and control over the information held about them, and help its institutions stay at the forefront of national and global privacy trends. The result is a law that is implementable, budget sensitive, and scalable across the public higher education institutions of the state.

ViziBLUE

The University of Michigan developed the ViziBLUE Guide to Personal Data to provide visibility into the student data practices at the university. ViziBLUE increases transparency for students regarding data collection, usage, and sharing within the university's IT ecosystem.

Institutions can take at least three basic steps to address student data privacy and governance. First, colleges and universities need to make student data privacy a priority, protecting student data by storing data securely, requiring MFA/SSO, and adopting strong password standards and practices. Additionally, higher education institutions should review current and new contracts to verify vendor compliance with regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). Preemptive moves by US institutions to comply with standards established by the European Union's General Data Protection Regulation (GDPR)—before they are required to—would signal a firm, long-term commitment to student data privacy. Further still, vanguard institutions could work with their state legislatures to craft student data privacy laws to protect personal information, giving students greater access to and control over the information collected on them, as the University System of Maryland has done.

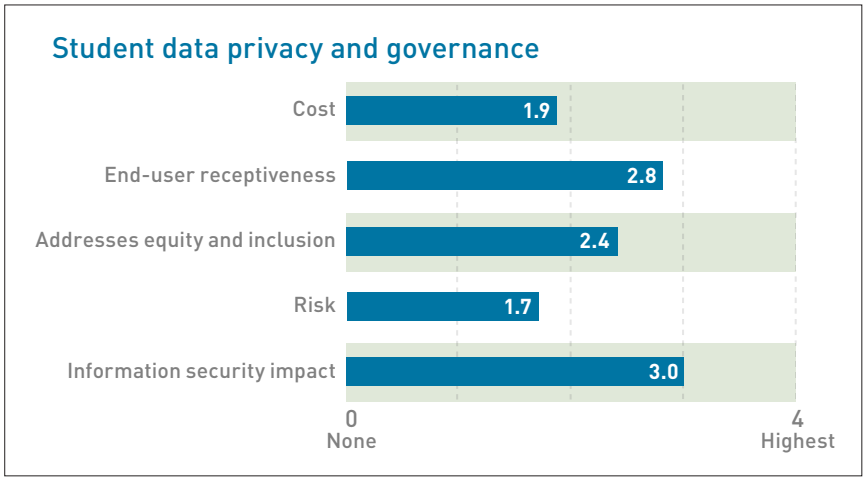
Second, institutions can be more transparent about how they handle personal student data by (1) disclosing to students what data are being collected and how those data are stored, used, and protected; (2) seeking informed consent from students about their data; (3) allowing students to review and update their own data on demand; and (4) giving students the chance to opt out of institutional data collection and usage at any time. The ViziBLUE program at the University of Michigan provides students with detailed information on what data are collected, how data are used, how data are collected, and how data are shared, with resources that students can use to take action or learn more.

Third, institutions can create campus-based information security awareness campaigns to help students keep abreast of current efforts to improve security, protect data privacy, and identify potential threats. Periodic security and privacy reports can go a long way to helping students stay informed so that they can make informed and proactive decisions about their personal data, thereby improving student confidence and trust in the institution. Begin these efforts with students as soon as they arrive on campus, as The Ohio State University Privacy Team did by hosting privacy workshops as part of the First Year Experience.

Does Anyone Care About Privacy Anymore?

In 2020, the Ohio State Privacy Team launched its inaugural session with the goal of having students practice thinking critically about privacy topics. Ninety-seven first-year students attended one of four sessions to learn about the Ohio State Privacy Principles and digital footprints and practiced conducting privacy impact assessments.

Relevance for Information Security



The Horizon Expert Panel is bullish on the potential benefits of student data privacy and governance to higher education. The potential impact of student data privacy and governance is high (3.0), and end users are likely to embrace it when adopted and promulgated (2.8). The panel even sees an opportunity to address some issues related to equity and inclusion (2.4) with the establishment of data governance and privacy protections for students' personal information. The costs (1.9) and risks (1.7) associated with security student data privacy and governance are seen as moderate.

Institutions may face some challenges as they endeavor to ensure student data privacy and establish data privacy governance. On a basic level, privacy initiatives and the tools that support them require human, financial, and technological resources that some institutions may not be able to afford presently. Furthermore, each institution will need to confront the tedious and arduous tasks of identifying the location and content of all of their data repositories that might be storing and using personal student information across campus so that the institution can actually honor student requests to opt out. Integrating data across systems and establishing the rules, definitions, and lines of accountability can be both time-consuming and expensive. Moreover, the work of identifying which data to collect (or not to collect) and establishing the rules for what may (or may not) be deleted is necessary for the institution to understand what it needs in order to carry out its work of educating and supporting students. And when students opt out of personal data collection, use, and storage—and they will—institutions need to be prepared to tweak their algorithms and/or find other ways to serve students who become invisible to or harmed by those algorithms. What is at stake is no less than the trust and confidence of the students whose data we collect and use to their benefit.

Further Reading

EDUCAUSE

The Evolving Landscape of Data Privacy in Higher Education

US Department of Education: Protecting Student Privacy

Protecting Student Privacy: Postsecondary School Officials

Purdue University Global

Cybersecurity Awareness for College Students: 7 Things to Do Now

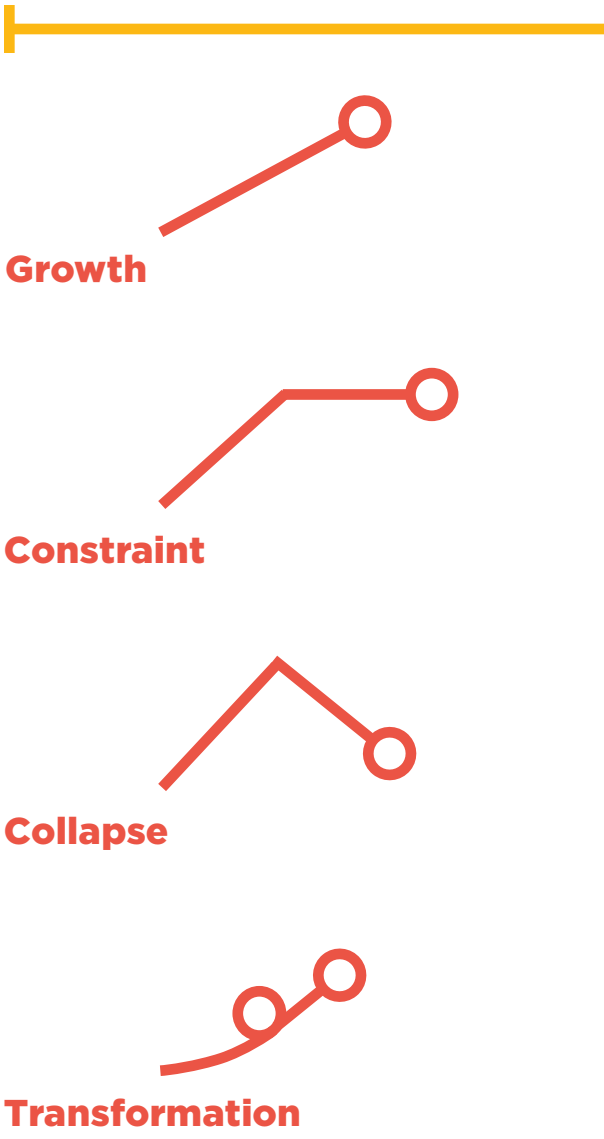
Scenarios

Today, planning for the future is probably as complex and as challenging as it has ever been. Given well-known challenges such as the pace of change and the unknowns of our post-pandemic outlook, planning needs imagination, flexibility, and a willingness to consider options from a variety of possible futures. Any action plan we formulate today is based on assumptions about what is likely to happen tomorrow. But if we lock our action plans too firmly to a specific set of assumptions, what happens if the future turns out differently, and those assumptions are not realized? Should that happen, then we may be pursuing a course of action that is out of sync with actual events and might even work against our interests.

Clearly, plans that enable us to navigate diverse futures are more robust than plans that are cemented to a single version of the future. In this section we synthesize and build on input from our expert panelists, using a tool from the Institute for the Future: envisioning alternative futures. By doing so, we can be both grounded and more imaginative in our planning and equip ourselves with the flexibility we need to encounter what does eventually occur. This section of the *Horizon Report* is an exercise in anticipating alternative futures for higher education.

We provide four such scenarios. Each is written from an imaginary viewpoint in the future, reflecting on the course of higher education through the decade of the 2020s. We are using the institute's four scenario archetypes or generic shapes of change. The first is growth, a scenario that takes current trajectories into a future in which the higher education cybersecurity profession has grown tenfold and campuses have increased focus on collaborative efforts to standardize collective approaches to cybersecurity. The second is constraint, in which higher education security professionals find themselves in a profession riddled with personal liability. Third is collapse, a scenario in which "security fatigue" has taken hold across higher education and the developed world and societal expectations of cybersecurity and privacy are nonexistent. Finally, the transformation scenario introduces the "war on cyberterror," with cybersecurity educational trajectories being subsidized by the government.

We have taken this "all four points of the compass" approach to provide distinct future alternatives. These archetypal scenarios will enable you to anticipate a variety of possible futures in your planning for what might come our way.



Growth

Cybersecurity professionals have become linchpins of institutions of higher education evermore dependent on an array of smart and connected devices and on constant and seamless network access both on and away from physical campuses. Ransomware and hacking are ubiquitous features and are taken for granted. Any institutional business plan worth its salt prioritizes "cyber risk" at the top of its list of factors for evaluating strategic plans and decisions. Institutional stakeholders from the chancellor down to the first-year undergraduate student are well versed on the risks of their technological environments and take steps to secure their devices and networks habitually and instinctively.

In this digital future, a bad guy is lurking in the shadows of every network and scratching at the windows of every device. Yesteryear's threat of nuclear warfare is eclipsed by the threat of digital destruction, and ransomware and security breaches are the boogeymen that keep institutional leaders awake at night. News feeds are splashed with headlines of a hacker's successful breach of a major US state university system, the most destructive and prominent higher education–targeted cybersecurity incident on record. It takes years for the system to fully recover operationally and financially, sparking widespread panic and the shoring-up of security and privacy capabilities across the higher education landscape. Thinktanks and institutional consortia emerge to focus collaborative efforts on securing the future of higher ed and developing standardized and collective approaches to cybersecurity.

On average, institutions' cybersecurity staff have expanded tenfold, and more institutions have a chief information security officer serving on their president's or chancellor's cabinet than do not. Cybersecurity degree programs evolve and proliferate to meet the future workforce demands of the burgeoning cybersecurity field. A campus tour for prospective students and their parents makes its way across the campus lawn to one of the most important destinations—the institution's cybersecurity office, where the staff boast about their cutting-edge technologies and initiatives for guarding students' data and privacy, and where eager parents inquire about cybersecurity internships and work placement opportunities for their children.

Students both on and off campus are wrapped in cocoons of personally owned devices and social networks that blur personal and educational uses. From digital and robotic assistants to virtual and augmented reality devices to wearable and biometric technologies, the web of endpoints of concern to the institution's cybersecurity unit has become exponentially larger, more complex, and more diffuse. Fortunately, end users' awareness of and appreciation for security and privacy has also grown exponentially, and institutions' faculty, staff, and students are positioned as partners in ensuring the institution's safety, rather than as barriers or risks to it. Cybersecurity capabilities have advanced alongside the end user as well, making each individual's safety monitoring far easier. Endpoint protection platforms (EPPs) have become smarter and more all-embracing, and authentication solutions have become seamless, to the point of being invisible.

As institutions' capabilities and needs in cybersecurity evolve and grow, so too do their relationships with solution providers and big tech companies. The demand for third-party solutions and support skyrockets, tipping the scale of market power and influence toward the solution providers and away from individual institutions. It falls to consortia and regional collectives of institutions to leverage enough power to exert influence on purchasing and contract negotiations and to ensure solutions' compliance with higher education policies, values, and needs. The increasing level of collaboration and collective planning and strategic decision-making across institutions creates new spaces and opportunities for peer-to-peer learning and fosters new innovations and models for the future of cybersecurity practice in higher education.

Constraint

A decade after the wide distribution of vaccines put an end to the global coronavirus pandemic of 2020–21, higher education cybersecurity continues to reel from the move to remote work, to struggle with smaller IT budgets and larger operating expenses, and to comply with a host of new federal regulations governing data protection and privacy. In these ways, the pandemic fundamentally and permanently changed how the risks associated with the work of higher education are addressed.

In addition to the decimation of faculty and staff positions resulting from the financial fallout of the pandemic, most higher education employees have not returned to campus, opting instead to continue working from home. A spate of mergers and acquisitions that dramatically reduced the number of viable colleges and universities furthered the ossification of the remote higher education workforce. Many institutions eliminated faculty and staff positions to avoid redundancies, increase efficiency, and reduce cost overruns. The shift to remote work and learning increased the need for information security professionals to defend against the constant assault on the now borderless networks created by remote employees and students. To compete with private industry for quality talent, colleges and universities have made relocation entirely optional, a move that reduced some costs (e.g., moving expenses, office space) and has allowed institutions to effectively recruit staff, even in economically depressed markets.

Higher education's creation of a remote cybersecurity workforce has not come without costs. Continued reductions in state funding and decreases in tuition revenues have had deleterious effects on IT budgets. The remote information security workforce needs institutionally provided devices and/or software secured by expensive licenses for endpoint security solutions. Additionally, many institutions also offer monthly reimbursements for expenses incurred from the use of personal devices, networks, and ISPs and to offset rising electricity costs that are resulting from so many people working from home.

The increased use of personal devices for work in the wake of the pandemic led to an unprecedented surge of security incidents. In addition to the Great Higher Education Hack of 2027, in which the personal data of more than one million students was stolen from twenty of the largest colleges and universities in the United States, weekly cyber attacks targeting higher education faculty and staff during the 2020s prompted the passage and adoption of some of the most comprehensive data privacy protection and cybersecurity regulations ever drafted. Although the new policies did not slow the rate of attempted hacks, the criminal and civil penalties meted out to those responsible, as well as those who were responsible for protecting the data, changed how information security operates.

To protect themselves from lawsuits resulting from data breaches, vendors now insist on contracts that are inordinately complex and require significant legal reviews and negotiations prior to formal acceptance, a costly process that undermines the ability of higher education IT to respond to institutional needs in an agile manner. Furthermore, the cybersecurity insurance field has experienced a boon as every higher education institution is required by federal law to carry general breach insurance. Many also opt for specific policies on each third-party contract in which sensitive data could be exposed. Additionally, many higher education information security employees take out personal liability insurance policies to cover them in the event that victims, vendors, or institutions hold them responsible for any role they might play in allowing a breach to occur.

Ironically, in their efforts to protect the private information of students, faculty, and staff, higher education security professionals enjoy no workplace privacy, even when working remotely. The devices and software provided to information security professionals are centrally managed and closely monitored to reduce the probability of individual user error compromising the borderless campus network. Moreover, institutions monitor all information security employee activity—down to the keystroke—using an elite task force of internal auditors and compliance officers who enforce institutional privacy policies. Many institutions have adopted a zero-tolerance policy for information security employee errors that put the personal data of those at the institution at risk, making a career in this field a high-risk, high-reward path. Organizational bloat is a looming threat, given that institutions keep adding layers of internal security to respond to the ancient question, "Quis custodiet ipsos custodes?" *(Who will guard the guards themselves?)*

Collapse

At most institutions, cybersecurity professionals have been relegated to marginal support and maintenance roles, with some institutions even moving to completely cut their internal cybersecurity functions. Big tech corporations reign supreme, wielding the lion's share of the authority and control in protecting higher education privacy and security. In negotiating contracts, ensuring compliance, and mitigating risks, the role for colleges and universities has diminished to a mere formality or, at best, is subordinate to corporate terms and interests and nation-state policies and restrictions. Devices and networks—both personal and educational—are everywhere and always "on," listening and gathering data. Public sentiment toward data privacy and protection has trended toward wholesale acquiescence to the inscrutable "cloud," and student data has come to be viewed less as a treasure to protect and more as a commodity to sell to help buttress financially strapped institutions.

Individual institutions, and even collectives of institutions, have ultimately failed in their efforts to stay ahead of and protected from bad actors, whose sophistication in hacking has advanced far beyond institutions' own solutions and security measures. Big tech giants are the sole remaining bulwark capable of standing against advanced security threats, and institutions relinquish more and more control over their own security in exchange for the relatively lower risk that these corporations promise. And the exchange works, at least for the institution's security. A CIO at a large northeastern US institution sits down at her desk with her morning coffee, her home office window looking out over a snow-speckled yard. Her inbox dings—a weekly report from a vendor detailing a lengthy list of averted security incidents. The message ends, "Thank you for trusting us with all your institution's security needs!"

International boundaries in higher education attainment have been redrawn in thick, bold lines, with rates of international student mobility reaching their lowest levels in decades. More data-restrictive regions in Asia and Europe have all but shut down student enrollments from outside their own borders, and US institutions are nearly emptied of international students from regions wary of the more laissez-faire approach to data protection adopted by many US institutions, as well as deference to corporate interests and practices that fail to live up to international standards. Nationalism and isolationism continue on an upward trend around the world, and international tensions further erode between major nation-states and regions. Against these nationalist impulses, new political movements crop up, advocating for greater international cooperation and improved global relations, with improved and increased international student exchanges one of several signature program priorities.

"Security fatigue" has taken hold across most developed regions of the world. The innumerable security risks across technologies, devices, and networks have left most consumers and end users numb to the ever-present specter of digital danger, and most have become passively resigned to handing over their security to whoever can ensure it and benefit from it. Devices are no longer manufactured with built-in privacy screens or features. GPS tracking is built-in and is nonnegotiable in most devices and smart technologies. A student walks across the campus lawn at dusk and her glasses light up with an advertisement from a local grocer. "We see you just purchased a veggie sandwich at Paul's Deli for dinner, and you've recently joined your school's fitness club. You should try our new low-calorie vegetarian ham deli slices, now on sale!"

It's a time of famine for cybersecurity professionals in higher education, as most of the security needs and jobs have dwindled or moved off campus to technology and communications corporations and other specialized solution and network providers. Small enclaves of institutions with "homegrown" security tools and solutions—some even still employing their own CISOs—thrive as self-proclaimed stalwarts against corporate overreach into higher education. Their veteran CISOs remember fondly their profession's days of feast, and they roll their eyes when their inboxes ding with advertisements from big tech selling the promise of security.

Transformation

The 2020–21 global pandemic fundamentally transformed how higher education functions and, therefore, how information security operates. The move to remote, online learning forced many institutions to expand or, in some instances, create online course offerings and to convert many staff positions to fully or flexibly online. Once the pandemic subsided, many students, faculty, and staff opted to remain online for their learning, teaching, and work, permanently expanding the borderless networks in need of information security protection. The plethora of personal networks and devices attached to college and university servers proved to be low-hanging fruit for cybercriminals, who opted for frequent, precision attacks with smaller rewards rather than complex exploits with larger payloads. The routinization of security incidents eventually proved to be too much of a strain on already limited information security resources, especially information security professionals.

To respond efficiently and effectively to cybersecurity threats from enemies foreign and domestic, higher education information security has adopted a more aggressive posture for surveillance, threat detection, and preemptive activities. With the successful implementation in the early 2020s of technologies such as machine learning/AI, bug bounty programs, endpoint detection and response solutions, deepfake detection, data verification, and research security, higher education garnered the attention of federal authorities who want to leverage the new tools for their own purposes.

National security agencies collaborate with higher education institutions, leveraging campus technologies, computing power, and know-how to combat threats. The formalization of these partnerships has effectively deputized higher education in the "war on cyberterror" that monitors, detects, and proactively and even preemptively targets hackers, terrorists, and other cybercriminals. Additionally, counterintelligence efforts work to dismantle and respond to weaponized social media, disinformation campaigns, and propaganda factories.

The increased surveillance that many describe as authoritarian gradually became incompatible/inconsistent with many privacy rules, so in the late 2020s privacy advocates and security officials parted ways. The operational concerns of security had been gradually hampered by compliance needs, a fissure that had emerged in the late 2010s when increased privacy concerns led to the adoption of GDPR-like restrictions with a host of legal requirements and protections. Chief privacy officers have established their own domains, bringing institutional research, IRB, and general counsel units under their control, while cybersecurity has moved into the realm of intelligence, counterintelligence, and law enforcement of networks, systems, and end users.

To meet the demand for a highly educated, skilled, and ubiquitous information security workforce, the government infused higher education with the investment to establish cybersecurity as an academic discipline. Larger, public doctoral institutions were among the first to establish entire undergraduate and graduate programs in information security to train professionals to make up for a general shortage in the information security workforce. Rivaling the most established business schools for enrollment and investment in their Masters of Information Security programs, the new cybersecurity programs aim to grow the pipeline by extending their reach into the K–12 space with junior cybersecurity programs and hacking competitions. To date, the biggest problem has been recruiting faculty who have both the field experience and academic expertise to cover all of the courses students need to take.

In parallel to higher education, the private information security field is also thriving. Many smaller institutions and those without high-performance computing capabilities are forced to outsource their cybersecurity to larger campuses. The number of cybersecurity vendors has proliferated to fill the gap for institutions that cannot afford to run their own.

The scramble to identify and source affordable security solutions is made more difficult by the fact that the computing power required to run the cybersecurity centers and cool the server farms is producing spikes in electricity costs. Wealthier institutions have been able to lease, purchase, or build their own power plants to cover the electricity demand, selling off any excess to local power companies to offset other costs. Additionally, the institutions that could neither afford to build their own security systems nor contract with private companies began to pool their resources via a spate of mergers and acquisitions; some of the larger and wealthier institutions moved to acquire other campuses and extend their reach to other regions.

Implications: What Do We Do Now?

As a first step in a strategic planning process, you collect and identify the trends, trajectories, and signals that shape the present and seem to have enough momentum to inform the future. Once you have constituted this picture, the next step is to step back and ask: What are the implications? How should they inform my plans for the future?

To explore the implications of this report's findings, we asked several members of the expert panel to identify the most important two or three implications for their own higher education context and discuss how these implications might play out. One thing you discover very quickly when working with a diverse panel is that not all the findings are equally relevant across institutional contexts. What for one context might be an acute issue (for example, data security for federal research contracts) might not be an issue elsewhere. Hence it is a valuable exercise to have panelists review the body of findings and identify the key implications for their own unique situation.

Of the seven essays collected here, two are about non-US higher education segments: Australia (Sawyer) and Canada (Novik). We have three by US authors, covering different segments in US higher education: baccalaureate institutions (Harris), research institutions (Corn), and university systems (Pesino). We have also included two corporate perspectives: Cicso (Romness) and Microsoft (Faehl). Obviously, seven essays do not come close to covering all the facets of higher education. Although these essays don't represent every viewpoint, their value lies in part in the perspectives on higher education that they afford. The reader can have a better sense of which issues are unique to a specific segment and which are shared across national and institutional boundaries.

> What are the implications? How should they inform my plans for the future?

Australasian Higher Education

Greg Sawyer, Director, Cybersecurity Program, CAUDIT

The new normal, new working environments, new threats, and new unknowns—the impact of the COVID-19 pandemic continues to affect the Australasian higher education sector, providing a challenge and focus in 2021 as the working culture shifts. While the term "new normal" evokes strong emotion, the pandemic has undoubtedly changed daily life and has significantly impacted the sector, with job losses approaching an estimated 15% (21,000 FTE positions) and institutions addressing an estimated shortfall between $3 and $4.5 billion. International student numbers by mid-2021 are forecast to be 50% below 2019 numbers, with applications for international student visas collapsing.

Returning to a pre-pandemic modified normal would be a mistake, as the sector has shown resilience in the face of adversity.

Returning to a pre-pandemic modified normal would be a mistake, as the sector has shown resilience in the face of adversity, changing the way we live, work, and interact. Three key challenges identified in the 2021 Information Security *Horizon Report* are (1) adapting to securing and supporting ongoing remote workers and students, (2) networks without boundaries impacted by the cybercrime growth industry, and (3) the political impact of legislation and deteriorating international relations.

In 2020, remote work and learning was a necessary reaction. In 2021, it provides an opportunity to be embedded as a way of operating and realizing ongoing benefit. With recovery to 2019 international student levels not expected until 2024, remote work and learning provide the capability to deliver cost savings and the potential for competitive advantage. This change will force institutions to reevaluate the existing campus footprint and capitalize on the breakthroughs in remote working and the shift to remote learning. The growing acceptance by students of online study offers an opportunity to review the mix of learning, the format for delivery, and the amount of time required on campus for a great student experience. Likewise, in a constrained cybersecurity resource market, the rise of the anytime, anywhere professional supported through remote working—where outcomes, not presenteeism, are the measure—is an opportunity for positive change in retaining cybersecurity subject-matter experts in a dynamic market.

The transition to networks without boundaries hastened following the lockdowns of the pandemic. The traditional campus security perimeter is gone, and remote working will be more the norm, as will learning that involves both on- and off-campus elements. Remote workers will be a focus of cybercriminals through 2021, as cybercrime remains a growth industry. Users requiring an immersive experience will drive the adoption of new technologies including 5G, Wi-Fi 6, and high-speed home internet services in the changed security perimeter. The rapid rise in targeted ransomware threats, deepfake everything, and weaponized AI will see security incidents become routine, if they aren't already. Options exist in addressing the omnipresent threat created through networks without boundaries. Cybersecurity is a best played as a team sport, working collaboratively together rather than competing in the sector. Password-less and biometrics access will continue to transition from the future to reality within institutions, as will changing the paradigm moving from threat management to threat hunting, continuing the journey into zero trust and endpoint protection.

Nation-state actors continued to evolve in 2020, targeting the sector's COVID-19 response and Australasian entities, while using crisis-themed lures to adapt and expand credential theft and malware delivery. In response to the increase in nation-state and cyber threats, the Australian government has commenced several legislative and government-based cyber and foreign interference activities, several directly focused on the higher education and research sector. In New Zealand, the government provided a line in the sand laying out New Zealand's view of how international law translates to state-sanctioned cyber actions. If the government actions are harmonious in applying a risk-based model proportionate to the risks enacted with the sector and funded appropriately, the sector will benefit. Increasing collaboration, improving the sharing of threat intelligence, and incentivizing cyber across the sector are key outcomes. Foreign relations continue to have effects on the sector, dampening the recovery of international student engagement in key markets and increasing risk of nation-state influence. Cyber policies, as well as adherence to the University Foreign Interference Taskforce (UFIT) guidelines, will remain a key focus in managing the risk.

The year 2021 will be another difficult one for the Australasia higher education sector, with borders closed, budgets constrained, and campus environments changed. The pandemic has created momentum that was previously unattainable, which will assist in addressing the implications of the 2021 Information Security *Horizon Report* findings. The initiatives of the Australasian Higher Education Cybersecurity Service (AHECS)—led by CAUDIT in partnership with the universities, AARNet, AusCERT, AAF, and REANNZ working collaboratively across the sector—will proactively help address the challenges and safeguard the intellectual property, digital assets, people, and hence the reputation of Australasia's universities.

Author Bio

Greg Sawyer, CAUDIT's Director of Cybersecurity Program, has over 20 years' experience across the sector working in various roles including security, infrastructure, faculty, and program and project management. He is a returned serviceman, serving for 11 years in the Department of Defence—Army, including operation service in Cambodia with the United Nations. He has participated on external advisory boards and presented at numerous conferences. He holds a Master of Business Technology (MBT) and graduated from the CAUDIT Leadership Institute in 2018.

Canadian Higher Education

Keir Novik, Chief Information Security Officer, Simon Fraser University

Canada is not a large country, although we like to think it is. Sure, we have a lot of land ("from sea to sea"), but we are few in number. We look outside our country to learn from others, reflect within our hearts, and take pride in trying to do better. We are defined by our history of First Nations and settlers, we acknowledge mistakes that we have made, and we see ourselves as having become stronger. Higher education in Canada is shaped by what we have learned and who we are, and it shares many of the same challenges as higher education in other parts of the world, much as Canada shares broader issues with other countries, no matter how different we may want to be. I cannot speak for all of Canada, or all of higher education, or even all of information security, but I contribute my thoughts here. As information security increasingly touches the daily lives of all people, so too do the concerns of society expand the horizons of information security.

Technology has the power to do great good, but it must be guided with care if it is not also to cause harm.

We sometimes speak of Canada as a mosaic, and this description is as true of our culture as it is of specific trends or subject areas. Take the privacy of information as an example. We have a Canadian privacy law, but it includes a provision that provincial privacy law takes precedence if it provides equivalent or better protection. So we have a mosaic of privacy laws across Canada, which causes no end of consternation among vendors. But many themes are repeated, and a pattern can emerge from the mosaic. The heart is there. As we reflect upon a turbulent year, we can take strength from an increased concern for information privacy. Technology has the power to do great good, but it must be guided with care if it is not also to cause harm. Within higher education, we have a responsibility to care for the information that is entrusted to us, whether for research or learning, and to contribute to the communities of which we are an inextricable element. Heartfelt respect for personal information is the most important part of that. As we collectively come to appreciate the value of data accumulated and held about ourselves and our behaviors, higher education must take a leadership role and help us reflect on the implications and on how we should be securing that data. This role is already shown in our institutional interest in data governance and steadily multiplying privacy impact assessments, but it needs to go beyond to reflect privacy first in everything we do.

Privacy and information security support the mosaic of diversity within our people as well. With control of our personal information, we can reflect on who we really are and not on who people say we should be. Given the confidence to discover ourselves privately, not having ourselves bared to critique and censure, we will develop as individuals. Building on that diversity, we can strive toward inclusion and equity for all people, regardless of who they are individually. But we must recognize that our society is a complex system into which prejudice has been built—both consciously and unconsciously. We have seen how personal information, collected with malicious intent or kept insecure, can be abused to hurt minorities through surveillance and disinformation. We must address the systemic injustice. Higher education must again take a leadership role, help us acknowledge the mistakes that have been made, and help us find a path forward. I cannot see the path we must tread or even the first steps, beyond imploring a heartfelt respect for each and every one of us.

So the concerns of society expand the horizons of information security. The final societal concern will indeed be final if we do not address it—our changing environment. Our world will, quite literally, change beyond recognition if we cannot find a solution to the harm we are doing to our mosaic of ecosystems. The increase in environmental volatility was painfully apparent this year, even as we were distracted by so many other concerns. What can we do? Higher education can help again with leadership, teaching the importance of sustained action, and with research and innovation to build new ways of living. As much as I love information security as a field, I do not see a specific solution that we can provide, beyond continuing to support the mission and vision of our institutions of higher education, enabling them to make a difference.

As information security increasingly touches the daily lives of all people, so the concerns of society expand the horizons of information security. Ask not what privacy can do for you, but what you can do for privacy. Recognize and confront systemic injustice. How can we afford to address climate change? How can we afford not to, when the future of our planet is at stake.

Author Bio

Keir Novik is responsible for the information security program for Simon Fraser University (SFU), with a mission of supporting the university's strategic vision by assisting the entire SFU community in the use of best practices for information security. Goals and responsibilities encompass a center of excellence, policy and governance, core services, awareness and education, and the incident response life cycle. His vision is to see the university community proactively engaged in information security. Novik obtained his PhD in computational physics from the University of Cambridge and is a Certified Information Systems Security Professional (CISSP).

US Baccalaureate

Emily Harris, Director of Cyber Security, Marist College

Relative to other types of US postsecondary institutions, baccalaureate colleges and universities are characterized by some unique attributes. Notably, 80% of students at these institutions are enrolled full-time, and for these students, colleges and universities not only provide learning but also offer numerous services, including residential housing, work opportunities, athletics programs, extracurricular activities, and health care. The full-time student depends on the college for a broad range of services that support their personal journey as well as their academic one.

Younger generations are aware of the potential implications of giving away private information and are increasingly likely to question the use of their data for services they must sign up for.

As a consequence, relative to students at other types of institutions, these students have a greater reliance on services and systems provided by the IT department. Beyond the requirements of using academic tools such as the LMS, online class registration, digital communications, and grade delivery, students and their digital lives are tethered to the institution. They must provide personal data for campus job applications and payroll, participation in fitness classes and club activities, engagement in on-campus social networks, and when using the campus network for entertainment and gaming consoles, which often requires registration and authentication. All of these activities are captured and logged electronically, which means the institution is responsible and accountable for a vast amount of electronic data.

The COVID-19 pandemic has increased the usage of digital platforms to facilitate a safe learning environment for students in this segment. Students now find themselves registering for dining reservations, providing personal data to on-site contact tracers, and, where surveillance testing is required, providing their data to third-party health providers as a requirement of their continued enrollment.

This environment of enhanced data collection comes at a pivotal time: incoming college students have an increasing awareness of data privacy due to widely publicized data compromises and their own individual experiences with breach notification. According to the Verizon Data Breach Investigations Report, 2020 saw 3,950 confirmed data breaches across all industries, and of those, 58% included a compromise of personal data. The reuse, sale, and compromise of personal data is commonplace, and this increased awareness has a direct impact on the ways in which students seek full transparency and control of their own information.

Research suggests that consumers are becoming more willing to trade their individual privacy for the services they want to use, going so far as to accept payment for the reuse or sale of their information. However, as a counterbalance, younger generations are also more aware of the potential implications of giving away private information and are increasingly likely to question the use of their data for services they must sign up for, such as those required by their educational institution. These students will often seek information about where their data is stored, how it is being used, and what the mechanisms are for restricting it. Put simply, students who are not given an explicit choice about whether their private data can be collected, processed, or stored are more likely to question the appropriate use of that data.

The EDUCAUSE 2020 Top 10 IT Issues identified information security strategy and privacy as the #1 and #2 issues, respectively, facing CIOs across all segments of higher education. According to Carnegie data, baccalaureate institutions have the least amount of government funding from grants and contracts. This can present a real challenge to addressing these top two issues, as these formal relationships drive legislative requirements, including adherence to standards and frameworks. Institutions with extensive government funding and contracts are subject to requirements and regulations tied to that funding. As such, non-baccalaureate colleges and universities have stronger data privacy requirements and more frequently adopt formal standards and frameworks—for example, NIST 800-171 is required for government-funded research. Although the implementation of standards and frameworks is not equivalent to functional and operational information security, the implementation of such requirements, when deployed broadly and deliberately, has a direct impact on reducing the overall institution's risk profile. Thus, baccalaureate institutions tend to lack the external pressures that can help move their information security programs into maturity, relying instead on internal pressures such as those from students, faculty, and administrators.

Baccalaureate colleges and universities should recognize these challenges and prepare to respond to these pressures. A number of actions can be taken. Create a culture of transparency in which policies and procedures around data collection, processing, and storage are well documented and communicated. Implement a training and awareness program to educate employees on the appropriate use of data and the legislative requirements that govern that use. Listen to students as they express their concerns and provide mechanisms for accommodating data privacy requests where reasonable and appropriate. Ideally, information security and data privacy should rise in institutional priority, with shared governance and appropriate financial support.

Author Bio

Emily Harris recently joined Marist College as the Director of Cyber Security. Previously, she worked for Vassar College, first as the Director of Networks and Systems and then as the college's first Information Security Officer. She received her BA in Historical Musicology from Barnard College and is CISSP certified. Her professional interests include the intersection of information security and the law, especially as it pertains to current and future data privacy legislation.

US Research-Intensive Institutions

Michael Corn, Chief Information Security Officer, University of California, San Diego

Few sectors of the economy have had the persistent impact that our research and teaching universities have had. Contributing more than $591 billion to the national GDP and educating 90% of patent holders, higher education in the United States has shaped not just our industry but the minds of those building the future. Internationally, American universities remain the gravitational center of research and education, attracting more than one million of the brightest minds from around the globe. It is precisely this outsized role that creates challenges for our sector. Geopolitical tensions trickle down and threaten to disrupt our global educational status, and the value of our research activities makes us targets for cyber espionage.

The success of our research mission depends on the open and ultra-collaborative nature of modern science.

The Challenge of Collaboration. The success of our research mission depends on the open and ultra-collaborative nature of modern science. From LIGO to the COVID-19 vaccine, science is a team sport involving multiple institutions if not multiple countries. As security professionals challenged to expand our scope into research cyberinfrastructure, we aim to imbue into research computing the lessons learned from enterprise security, all the while protecting the creativity and agility of our researchers. Yet many of our traditional tools are frustrated by the distribution of resources among collaborators. For example, how do we ensure that appropriate background screening has taken place for collaborators accessing local cyberinfrastructure? How can we ensure that remote endpoints and networks meet local requirements? Surely the path forward is to work collaboratively ourselves, as the identity community has for federated access.

Networks without Borders. A closely related challenge is the notion of infrastructure without borders. Since the ascendency of cloud computing, our traditional construct of a network perimeter, or even the "internal" network, has been eroded and replaced with the establishment of a permeable border. For enterprise computing, this is seen through a growing dependency on SaaS services. For these services, we are largely shifting responsibility (and liability) for security to third parties through contract vehicles. However, for research cybersecurity in which the infrastructure is supported through a hybrid of shared local, remote, and cloud resources, the models for securing this infrastructure are immature, particularly when involving regulated data. Examples of such projects are the Open Science Grid or the Pacific Research Platform. This remains an area of urgent research.

The Challenge of Regulation. Whether one is referring to the looming imposition of CUI from the Department of Education or the present challenge of the DoD's Cybersecurity Maturity Model Certification (CMMC), the burden of regulation is growing. For researchers unaccustomed to working under a regulatory scheme such as CMMC, the challenges are both practical (budgets, staffing) and cultural. Though it is easy to be diverted by the former, it is the latter—changing the relationship between researchers and security professionals—that will be the most challenging for research institutions. Many institutions are working on this issue, for example by attending the ResearchSOC workshops sponsored by the NSF or expanding support for research facilitation.

The Backdrop of Societal Unrest. Hypothesis. Predictions. Data. The spine of the modern liberal education is the scientific method. What we have experienced as a nation, however, is the triumph of the politics of disinformation as a counterbalance to science, amplified through the weaponization of social media. We feel adrift and disarmed as the usual instrument of thoughtful analysis falls away under the onslaught. As climate scientists have discovered over the past decade, simple and unquestionable data is rendered moot when confronted with identity politics. For research universities, this social unrest adds a new dimension of threat actors: those seeking to undermine data so as to discredit the underlying science. Thus, there is growing awareness that even open, publicly available data needs to address data integrity. Without data integrity, reproducibility is lost, and with it the scientific method.

Finally, I'd like to turn to a much broader challenge we face—the dilemma of privacy. As with the population in general, our community's expectations for privacy continue to grow. Concerns about corporate or authoritarian surveillance trickle down to students and staff, surfacing as skepticism in our own handling of personal information. How we meet those expectations will challenge us to go beyond mere questions of data access. As we turn to correlating human behavioral data with institutional academic and business data, the engine of modern analytical techniques will produce both startling insight and considerable discomfort. Will we rise to the challenge of shaping the boundaries of such analysis? Privacy of thought and in communication forms part of the cognitive framework that supports human social and intellectual activities. Benefiting from contemporary analytical power while addressing privacy expectations will require a deep exploration of privacy as a feature of university life, not merely as oppositional to corporate or authoritarian surveillance.

This report identifies a number of challenges, many of which can be seen along various dimensions, of which research security is only one. However, I strongly encourage universities to recognize that addressing research cybersecurity is fundamentally different from the enterprise security we've grown accustomed to. Exploring how to organize and resource research cybersecurity requires its own analysis and strategy. Institutions of higher education have been a persistent feature of human culture for at least a millennium. Yet the context in which we operate is one of change: economic, intellectual, cultural, and political. As institutions, our primary challenge is, as always, to ensure our own operations are tuned to the influences of society at large.

Author Bio

Michael Corn is the Chief Information Security Officer at the University of California, San Diego. He is a former co-chair of the Higher Education Information Security Council and is currently a member of the REN-ISAC steering committee. He is a frequent author on topics of security, privacy, and identity management and is senior personnel on NSF Grant 1840034 "ResearchSOC."

University Systems in the United States

Sherry Pesino, Information Security Program Administrator, Connecticut State Colleges and Universities

Different types of university systems exist in the United States. Some systems reflect private and military institutions that are spread across the country. However, most of these are state university systems. These organizations are made up of state universities, state community colleges, or in some cases a combination of university and community colleges. Future trends and key practices in information security will impact university systems, and I focus here on the areas of network boundaries, escalations in security incidents, and the impact of data privacy laws.

The sheer number of machines that are now necessary makes the management of these devices cumbersome.

Traditional institutions of higher education have a network boundary that is typically the same as their physical footprint—the size of the campus. University systems have a naturally large network boundary based on how many institutions are in their state or across state boundaries. The COVID-19 pandemic and the work-from-home model have pushed the network boundaries for all institutions across continents. No longer are we securing the machines on our networks; meanwhile, the potential for BYOD use in the business functions of our institutions has increased. We now have functional staff using their family PCs to conduct business, with access to data that could be at a high classification level. The boundary of our networks is not just where the data is stored but also where it is accessed. With the work-from-home model, those locations could be anywhere. Many institutions have provided staff with university-owned machines that can be properly configured for the level of security needed. This includes providing machines to part-time employees and student workers. The sheer number of machines that are now necessary makes the management of these devices cumbersome. Incorporating endpoint detection and response for all the additional devices is difficult. Adding to the immense nature of these challenges are the types of attacks that take place daily.

According to the 2019 Internet Crime Report from the FBI Internet Crime Complaint Center, phishing/vishing/smishing/pharming attacks made up the largest number of cybercrime victims in 2019—more than 110,000. Business email compromises (BEC) and email account compromises (EAC) complaints saw losses of $1.7 billion. Although final reports for 2020 are not currently available, the number of victims and costs are expected to be much greater. The pandemic has opened an opportunistic window for cybercriminals. The Connecticut State Colleges and Universities System has seen an uptick in phishing attacks, and as a result, user accounts are becoming compromised. Couple that with the sudden shift to a remote work environment, and you have the perfect storm.

This increase in incidents means more resources are focused on reacting rather than preventing. We are unable to get ahead of the threat actors. Cybercrime is up 600% due to the pandemic, and because most malware is delivered by email, our inability to respond efficiently to these attacks will inevitably mean more victims and more financial losses. Another consequence of this increase in incidents is the inability to effectively protect individuals' data privacy. The past three years have seen an increase in privacy regulations, focused not only on student data and privacy but also on the governance of everyone's data and privacy rights. The European Union's General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA) 2020 are just the starting points for requirements to protect individuals' data.

From the federal level to the states, data privacy laws require institutions of higher education to implement privacy governance models, leading to the need for a leadership role in data privacy. In many institutions this role was a function of the chief information security officer, but the added level of complexity for university systems requires these responsibilities to be managed by an office of its own.

University systems are typically state funded. They have many federal ties through research and financial assistance, and they maintain a significant number of individual data elements in their data systems. These data systems must communicate with each other across multiple university system institutions. As the Connecticut State Colleges and University System is learning with the merging of its 12 community colleges into a one-college model, admissions data and academic data must be made available across the 12 campuses versus being managed in one location. The pandemic has also added another layer of complexity—staff of the admissions office and the registrar's office are all working from home. Sharing data across the department while maintaining privacy of the data is not as simple as walking to a colleague's cubicle.

The ongoing challenges presented by the multitude of schemes and ploys of cybercriminals have only been compounded by the COVID-19 pandemic. It is imperative that the security of our information systems be as adaptive and comprehensive as possible to ensure the integrity of our university system networks.

Author Bio

Sherry Pesino is the Information Security Program Administrator in the CSCU Information Security Program Office (ISPO). Her responsibilities include developing security standards and procedures for the university system, which includes 17 separate institutions. She has the role of Information System Security Officer (ISSO) for the 12 community colleges, including incident investigations and the Information Security Awareness Program. Her journey to information security started with teaching elementary school and working in educational and instructional technology for 14 years at a state university. For the past 6 years in the ISPO she has been given the opportunity to earn her CISSP and participate in the rollout of a progressive, updated information security program.

An Industry Perspective on Securing University Research

Peter Romness, Cybersecurity Principal, Cisco US Public Sector CTO Office

We've seen in the news that opportunistic cybercriminals and nation-state actors are targeting COVID-19 vaccine and treatment research. Although these attempts to steal intellectual property or disrupt progress are newsworthy, pandemic-related information is not the only research at risk. According to the NSF, total university-performed R&D surpasses $55 billion a year, and the sad truth is that all such research is increasingly under attack by hackers.

> As vendors, we should be there to roll up our sleeves and help you implement an effective cybersecurity environment that meets your specific requirements.

Cyber defense was never easy, but this focus by cybercriminals and the nature of the higher education environment makes it particularly challenging to protect research environments. Vendors offer many kinds of tools to help you defend your lab, but we need to do more. We need to work with you to help you decide which tools are right for you and to make sure that they all work together to protect your environment and help you quickly respond to any threats.

Unique Challenges for University Research

What makes research a target? To paraphrase Willie Horton, "That's where the money is." Your researchers are developing valuable data that criminals can sell and nation-states can use to gain advantage. Several other unique challenges likely also make your institution attractive to hackers:

- Your users like the feel of an open environment, so you need to give them easy access to the information they need and allow them to share while protecting them from threats.
- You have a large volume of sensitive data, which is usually housed in the individual research labs or even on an individual researcher's computer. This dispersed architecture can provide multiple paths to exploit vulnerabilities.
- Many personal devices are connecting to your networks and probably have sensitive data on them. Your researchers could be putting valuable research at risk when they engage in activities such as checking their email while on public Wi-Fi.

Your research labs might also be subject to requirements as a condition of receiving grant funding. Given that 60% of research funding in the United States comes from the federal government, the Cybersecurity Maturity Model Certification (CMMC) is looking like it will be the toughest of those requirements. The Department of Defense is starting to require it for their contracts, and civilian agencies are talking about using it too. It is based on NIST SP800-171 capabilities but adds requirements from the Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations (DFAR). Moreover, you can no longer self-certify that you meet the requirements; to bid for funding, you must be certified by an approved auditor.

The Role of the Technology-Solution and Service-Provider Community

The path you take to defending your research will depend on your goals and the needs of your researchers. As vendors, we should be there to roll up our sleeves and help you implement an effective cybersecurity environment that meets your specific requirements, not just sell our products. Recommended steps to do this include the following:

- **Assess where you are and develop a planned end-state.** Vendors should work with you to help develop your security goals, provide expertise and tools to help you understand your current environment, and then help you develop your future security architecture.
- **Use best practices and requirements.** As you make your plan, guidelines such as the CIS critical 20 or the NIST Cybersecurity Framework (CSF) are widely used ways to make sure you are addressing all the risk factors. If you're handling personal data, you may want to look at NIST SP800-171, and if you have federal grants, you should start looking at the additional FAR and DFAR clauses of CMMC.
- **Look for quick time-to-value.** Look for tools that, because they are easy to implement and cover large security gaps, allow you to move toward your goals and show quick results. This could be something like DNS protection that prevents users from surfing to websites that serve up malware or provide backdoors to criminals. Another fast win is multifactor authentication to protect against credential-theft account takeover.
- **Think "cloud smart."** Cloud security and cloud apps can help you get things up and running faster and can be easier to manage, but they can get expensive and may not be right for every situation. Weigh your options and make sure your choice fits into your long-term security architecture plan.
- **Demand integration and automation.** Stand-alone or hard-to-integrate security tools no longer have a place. Any tool that you add to your environment should communicate with all the others and be easily managed. You should be able to see what's going on in your environment and be able to take quick action when needed.

Protecting your lab data from cybercriminals is hard but critical to your success. Vendors should be proud to help you meet your goals while deploying effective security, not just sell you products.

Author Bio

Peter Romness is responsible for engaging US federal, state, local, and education institutions to inform the development of Cisco's Public Sector solutions. He's been helping government and education organizations securely accomplish their goals for over 30 years. Prior to Cisco Systems, Romness held leadership positions at Hewlett-Packard, AT&T, and Panasonic. He holds a degree in mechanical engineering from Duke University.

Industry Contributions to Information Security

Steve Faehl, Security CTO, Microsoft US

In 2020, for many educational institutions the ability to work and learn from anywhere transitioned from a lofty and seemingly faraway ideal to an existential imperative. In this era of remote everything, we have seen organizations accelerate and realize two years' worth of digital transformation in just two months. Cloud vendors enabled the rapid rate of this massive shift in adoption of technology, with high availability at scale and ease of onboarding being the primary driving factors. Over time, additional priorities emerged as remote digital activities and the technologies that enabled them became the primary experience for higher education communities. As institutions' technology adoption rose, so did their expectations of the quality and security of the digital campus experiences they depend on.

> While accelerated digital transformation has brought both benefits and challenges to higher education institutions, their cybersecurity needs are at an all-time high.

Rapid adoption of new technologies can easily outpace the ability of information security teams to effectively secure them, leading to blind spots and compromise or disruption by cybercriminals. In an effort to drive increased adoption through easier user experiences, vendors, IT teams, or end users often relax security controls. Vendors can help remedy this with designs that are "secure by default" and by providing granular security policies. Any options configurable by end users that have security or privacy implications should also be called out in plain language, facilitating predictability and trust. For example, Microsoft Teams introduced an option to prevent unwelcome meeting guests with "by invitation only" meetings, providing an easy way for meeting organizers to manage attendees upfront, keeping a secure meeting experience simple and understandable. Technology vendors should also endeavor to be prescriptive in publishing security best practices. Microsoft has experienced great success with the inclusion of the Secure Scores product, which enables security teams to get up to speed quickly, assess gaps, and prioritize areas for improvement. Also essential is that vendors maintain their own robust threat detection, insider threat, and supply chain assurance programs, given that increasingly sophisticated attackers seek to use compromised vendors to achieve broad, persistent access to their client base.

Some security teams have fallen behind due to the increased digital footprint, which provides more opportunities for cybercriminals, and because remote access can reduce visibility when there is an overreliance on network-based detections and controls. Cloud-based security tools can help keep pace with rapid change by achieving ROI more quickly. However for security teams, learning to use new tools can be disruptive, giving adversaries a temporary advantage. Vendors should prioritize interoperability and side-by-side operation to reduce risk during transition. In addition to faster adoption timelines, cloud-based security tools often benefit from rapid detection updates and integrated threat intelligence at scale, which can provide a significant advantage for defenders. To overcome reliance on network detections, vendors and organizations should pivot to include endpoint, identity, and application security controls.

Whereas identity has been central to higher education for many years, cloud-based identity can provide additional flexibility and resilience. Additionally, enhanced detection and response (EDR) has emerged as an essential capability, allowing for centralized investigation and filling in network visibility gaps. There are two important areas for security vendors to pursue for EDR offerings for higher education. The first is to extend detection and response capabilities (XDR) beyond endpoint-only data to include email, identity, application, and network, which greatly reduces integration work. The second is to include artificial intelligence and automation to reduce false positives and lower incident response time. These features empower security teams by reducing their workload and eliminating unnecessary noise. This approach has enabled customers to increase their SOC efficiency by 87% or more and reduce analyst alert fatigue by up to 90%. As XDR solutions continue to mature, we also expect automated blocking and mitigation attempts to be superseded by more advanced self-healing techniques that analyze impacted resources against known-good states and return the resources to health automatically.

While accelerated digital transformation has brought both benefits and challenges to higher education institutions, their cybersecurity needs are at an all-time high. Higher education is a prime target of cybercriminals due to the high ratio of devices/users to security team members, vast stores of personally identifiable information, and valuable research data. In the second quarter of 2020, 63% of malware sightings worldwide were targeted at the education industry. Vendors need to better support higher education with "secure by default" designs and cloud-based tools that include prescriptive security best practices. Vendors also need to ensure that they maintain robust internal security and compliance practices to further reduce risk to their clients. Vendors creating security tools should maximize interoperability and broaden their scope beyond a single domain such as network or endpoint while empowering security professionals with automated investigations and self-healing to provide a cleaner pane of glass. As a result, higher education will be able to maximize flexibility with secure remote work and learning options while also becoming more resilient against cyberattacks.

Author Bio

As Microsoft US Security CTO, **Steve Faehl** leads the Microsoft US security business and shapes its strategy by identifying and evangelizing the most valuable cyber defense tactics available to organizations today. Faehl works with Microsoft customers across all US verticals from education and government to retail and financial services to ensure that Microsoft's approach to security remains pragmatic based on real-world customer evidence. He coordinates with internal security experts from every area of Microsoft, giving him a unique view of both industry needs and Microsoft's capabilities to address them. Faehl also leads several cyber R&D efforts in pursuit of new security features and strategies to disrupt emerging cyberattacks.

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 industries. The members of this year's group, all first-time Information Security Horizon panelists, were sought out for their unique viewpoints, as well as their contributions and leadership within their respective domains. The panel represents different global contexts, with members contributing from the United States, Canada, and Australia. 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 year's expert panel research followed a modified Delphi process, in addition to adapting important elements from the Institute for the Future (IFTF) foresight methodology. Following the Delphi process, our expert 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 information security 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 minimal influence on the content of the panel's inputs and discussions. This was done to protect the core intent of the Delphi process—that an organized group of experts themselves discuss and converge on a set of forecasts for the future, based on their own 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 on the IFTF trends framework and process for collecting "signals" and "impacts" for trends. Ensuring an expansive view across all the many factors influencing the future of higher education, the IFTF "STEEP" trends framework enabled our panel to focus on **S**ocial, **T**echnological, **E**conomic, **E**nvironmental, and **P**olitical trends. This effectively broadened the panel's input and discussions beyond the walls of higher education to more explicitly call attention to the larger contexts within which information security practices take place. 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 emerging information security technologies and practices.

As they provided their inputs and engaged one another in discussion, panelists were encouraged to share 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 forecasts are sufficiently grounded in "real" data and trends, not merely science fiction.

Panel Questions

The following questions were designed to elicit an open range of responses from the expert panel and then to narrow those responses to a consensus through rank-order voting. Voting on trends was done separately for each of the five STEEP trend categories: social, technological, economic, environmental, and political.

STEEP Trends

Round 1 (for each STEEP trend category): Provide evidence/signals of each trend and detail the impact you believe that trend will have on the future of higher education information security.

Round 2 (for each STEEP trend category): The list below summarizes the 12 most influential trends, as selected by the Horizon panel. From this list, please rank order what you believe will be the three most influential trends for the future of higher education information security.

Key Technologies and Practices

Round 1: 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 higher education information security. Include with each tech or practice, if possible, a brief explanation of why you believe this tech or practice will have a significant impact on the future of higher education information security, as well as an example that comes to mind of a program or institution that exemplifies this key tech or practice.

Round 2: Please select the top 12 techs and practices you believe will be most impactful for the future of global higher education information security.

Round 3: Panelists provided ratings on the following dimensions for each of the top six techs and practices:

- Do you anticipate the adoption of <tech/practice> will require new kinds of literacies on the part of information security professionals?
- How useful will <tech/practice> be in helping institutions address issues of equity and inclusion in information security?
- Thinking about the evidence currently available, how would you rate the potential of <tech/practice> to have a significant and positive impact on overall institutional information security?
- Thinking about the probability that this tech or practice will succeed at the institution, how would you rate the level of risk involved in adopting <tech/practice>?
- Overall, how receptive would you say end users (e.g., faculty, staff, students) would be to adopting <tech/practice>?
- Relative to institution size and budget, how much institutional spending would you anticipate would be required to adopt <tech/practice> across the institution?

Expert Panel Roster

Brian Kelly
EDUCAUSE
Director of the Cybersecurity Program

Mark McCormack
EDUCAUSE
Senior Director of Analytics and Research

Jamie Reeves
EDUCAUSE
Product and Portfolio Senior Manager, Communities and Research

D. Christopher Brooks
EDUCAUSE
Director of Research

John O'Brien
EDUCAUSE
President and CEO

Frank Barton
IT Systems Administrator
Husson University

Sol Bermann
CISO & Executive Director of Information Assurance
University of Michigan

Chris Bernard
CISO
University of Connecticut

Eric Berube
Senior Director and Chief Information Security Officer
Bowdoin College

Cara Bonnett
Senior IT Analyst and Team Lead
Duke University

Alan Bowen
CISO
Franklin & Marshall College

Michael Corn
CISO
UC San Diego

Juan Cruz
Information Security Manger
Guilford Technical Community College

Niranjan Davray
Chief Information Officer
Colgate University

Jason Edelstein
IT Risk and Compliance Program Manager
University of Chicago

David Escalante
Director of Computer Policy & Security
Boston College

Steve Faehl
Security CTO
Microsoft US

Scott Fendley
Information Security Architect
University of Alabama at Birmingham

Ricardo Fitipaldi
Interim CISO
San Diego State University

Rebecca Fowler
Interim Chief Information Security Officer
University of Missouri

Joanna Grama
Associate Vice President
Vantage Technology Consulting Group

Chris Gregg
CISO
University of St. Thomas (Minnesota)

Emily Harris
Director of Cyber Security
Marist College

Rick Haugerud
Asst. VP for IT & CISO
University of Nebraska

Leo Howell
CISO
University of Oregon

Tomomi Imamura
Team Lead—Security Testing and Cyber Defense
University of Wisconsin–Madison

Robert Lau
Director, Information Security Architecture
University of Southern California

Nick Lewis
Program Manager for Security and Identity
Internet2

Douglas Lomsdalen
Information Security Officer
California Polytechnic State University

Randy Marchany
CISO
Virginia Tech

Ben Marsden
Information Security Director
Smith College

Kim Milford
Executive Director
REN-ISAC (IU)

Jeff Miller
Director, Information Security & Infrastructure
University of Central Oklahoma

Matt Morton
Senior Strategic Consultant
Vantage Technology Consulting Group

Keir Novik
Chief Information Security Officer
Simon Fraser University

Patty Patria
Vice President for Information Technology & CIO
Worcester Polytechnic Institute

Marden Paul
Director Planning Governance Assessment
University of Toronto

Sherry Pesino
Information Security Program Administrator
Connecticut State Colleges and Universities

John Ramsey
Chief Information Security Officer
National Student Clearinghouse

Peter Romness
Cybersecurity Principal, Public Sector CTO Office
Cisco

Greg Sawyer
Director, Cybersecurity Program
CAUDIT

Jamie Schademan
Chief Information Security Officer
Central Washington University

Sandy Silk
Director, Information Security Education & Consulting
Harvard University

Tom Siu
CISO
Michigan State University

Damien Smith
Cyber Security Analyst / Adjunct Faculty
Dallas College

Marti Snyder
Professor
Nova Southeastern University

Ernie Soffronoff
IT Director
Whiting School of Engineering, Johns Hopkins University

Andrew Sroka
President and CEO
Fischer Identity

Michael Stamas
Co-Founder & VP
GreyCastle Security

Chad Tracy
Director of Information Security, Privacy, and Compliance
Bates College

Jerry Tylutki
Information Security Officer
Hamilton College

Marcos Vieyra
Associate Vice President and Chief Information Security Officer
University of South Carolina

John Virden
CISO
Miami University

Cheryl Washington
CISO
UC Davis

Jason Williams
Director, Information Security and Compliance
University of Notre Dame