Have you read *The 2021 EDUCAUSE Horizon Report | Information Security Edition*?

a) Yes! Cover-to-cover! And twice!
b) Yes, but only if you won’t ask me any questions about it.
c) Yes, bits and pieces
d) No, but I’ve downloaded, printed, &/or forwarded it to others.
e) No, but I’m going to as soon as we’re done here! Promise!
f) Wait....what’s a ”Horizon Report”? 
The 2021 EDUCAUSE Horizon Report
Information Security Edition
https://tinyurl.com/2021InfoSecHz

The 2021 Horizon Report Team

D. Christopher Brooks, Director of Research

Greg Dobbin, Senior Editor

Brian Kelly, Director of the Cybersecurity Program

Mark McCormack, Senior Director, Analytics and Research

Jamie Reeves, Product and Portfolio Senior Manager, Communities and Research
Sense-making

Dennis Gabor, Inventing the Future, 1971

“The future cannot be predicted, but futures can be invented.”
Prediction vs. forecast

The future vs. many possible futures
5 principles à la Gorbis

1. Forget about predictions
2. Focus on signals
3. Look backward to look forward
4. Uncover patterns
5. Create a community
Trends

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

Uber Trend: Remote Work

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
Social Trends

The world is constantly changing and evolves, so too do our needs for more, better, and different approaches to information security. Our patterns of human behavior and the social environment in which we find ourselves shape how we interact with the technologies and systems we use, and they also shape the ways in which we must protect these technologies, these 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 well 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 workforces, but the labor market also demands that workers, both inside and outside higher education.

Evidence: The US Bureau of Labor Statistics has estimated that the demand for “information security analysts” will grow 36% from 2019 to 2029, and yet the pool of talent for these jobs is falling, with fewer students majoring in information security.

Greater Focus on Data Privacy

Impacts: The proliferation of personal devices and individual interactions continue to create the awareness and importance of individual data privacy, increasing the boundaries of institutions’ use and 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 US Bureau of Labor Statistics has estimated that the demand for “information security analysts” will grow 36% 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.

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 well 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 workforces, but the labor market also demands that workers, both inside and outside higher education.

Evidence: The US Bureau of Labor Statistics has estimated that the demand for “information security analysts” will grow 36% from 2019 to 2029, and yet the pool of talent for these jobs is falling, with fewer students majoring in information security.
Key Technologies & Practices

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

What kinds of challenges might institutions encounter if they go forward with any of the technologies or practices identified in the report? To assess the nature and extent of the impact of these key technologies and practices, we asked panelists to rate each of them across several dimensions, using a five-point scale (1 = none, 5 = 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 likelihood?
- How acceptable will it and users (e.g., faculty, staff, students) be to adopting it?
- What level of institutional buy-in 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

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

EDUCATEA’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.
Cloud Vendor Management

Cloud Vendor Management in Practice

Relevance for Information Security

Cloud vendor management

<table>
<thead>
<tr>
<th>Cost</th>
<th>1.9</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user receptiveness</td>
<td>2.1</td>
</tr>
<tr>
<td>Addresses equity and inclusion</td>
<td>1.9</td>
</tr>
<tr>
<td>Risk</td>
<td>1.7</td>
</tr>
<tr>
<td>Information security impact</td>
<td>3.1</td>
</tr>
</tbody>
</table>

None Highest

Cloud Vendor Management

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. The Berkeley Leadership reviews HECVAT responses in conjunction with a supplier security plan and supplemental documentation (e.g., SOX 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.

Further Reading

EDUCAUSE Review
Tying Up Loose Ends in Transitioning to the Cloud

EDUCAUSE Review
Rowing Together, Vendors and CIOs Navigate Tricky Relationships

This has been approved for publication on a certain technology platform. The EDUCAUSE Purchasing Department and the Office of General Counsel are currently reviewing an initial draft of a document. The final product may be slightly different from what is currently available. We will outline any changes and updates here.

Information security impact

None

0

4 Highest
Any 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 uncertainty of our post-pandemic outlook, planning needs imagination, flexibility, and 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 set out acting plans too firmly in a specific set of assumptions, what happens if the future turns out differently, and those assumptions are not realized? Indeed, that happens, then we may be presenting a source of action that is not of course with actual events and might even work against our interests.

Clearly, plans that evolve to accommodate diverse futures are more robust than plans that are conceived by a single view of the future. In this section, we synthesize and build on input from our expert panel, using a well-known framework for the Future: envisioning alternative futures. By doing so, we can for both grounded and more imaginative in our planning and apply ourselves with the flexibility we need to recognize what does eventually occur. This section of the framework is an exercise in synthesizing alternative futures for higher education.

We provide four such scenarios. Each is written from an imaginative viewpoint in the future, reflecting on the course of higher education through the decade of the 2020s. We are using the scenario's flow to see narrative, metaphor, or gestalt shapes of change. The first is growth, a scenario that takes current trajectories into a future in which higher education cybersecurity professions have grown robust and campuses have increased focus on collaborative efforts to establish collective security in cybersecurity. The second is constriction, in which higher education cybersecurity professions find themselves as a profession ratified with personal liability. Third is collapse, a scenario in which “security fatigue” has hit critical mass, and the higher education leadership and staff are depleted and unable to respond. Finally, the transformation scenario introduces the “self-sustaining” model, with cybersecurity educational resources being allochonous and generated by and through.”

We have taken the “all four points of the compass” approach to provide distinct future alternatives. These disciplinary scenarios will enable you to anticipate a variety of possible futures in your planning for what might come out today.
Implications
As a first step in a strategic planning process, you collect and identify the trends, potential, and signs that shape the present and seem to have enough momentum to inform the future. Once you have constructed 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, 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 those 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 country might be an urgent issue for another, the security the federal research community 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 systems: Australia (Sydney) and Canada (Nordia). We have these by US author, covering different segments: US higher education, baccalaureate institutions (Harvard), research institutions (Cornell), and community systems (Pima). We have also included two corporate perspectives: Cisco (Rutgers) and Microsoft (Fulbright). 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 then 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?
Connect with panelists and exemplars

University Systems in the United States

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

According to the 2020 Security Breach Report from the FTC, internet service providers (ISPs) are the second most common source of data breaches, just behind retail companies. Although data breaches in 2020 are not currently available, the number of attacks and their impact on the network proves.

The potential for PDDO in the business environment of modern organizations to protect the network from the breaching vector of cyber attacks.

According to the Business Insider, the average cost of a data breach for a company is $3.86 million, which is a significant cost for any organization. This cost is not only due to the direct financial impact but also to the damage to the company's reputation, which can lead to loss of customers and revenue.

The current data breach trends are not just focused on stealing data but also on utilizing the stolen data to perpetrate financial fraud. This trend is not only impacting businesses but also individuals.

The current landscape of data protection and privacy regulations is complex and evolving rapidly. Companies must stay informed and proactive in implementing the necessary safeguards to protect their data and comply with the various regulations.

In conclusion, protecting data is a continuous effort, and organizations must stay vigilant and proactive in their data protection strategies.
The sheer number of machines that are now necessary makes the management of these devices cumbersome.
The success of our research mission depends on the open and ultra-collaborative nature of modern science.

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.

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).

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.
On the Horizon for 2021

Thank you!

Jamie Reeves
(jreeves@educause.edu)

Mark McCormack
(mmccormack@educause.edu)

Brian Kelly
(bkelly@educause.edu)

D. Christopher Brooks
(cbrooks@educause.edu)