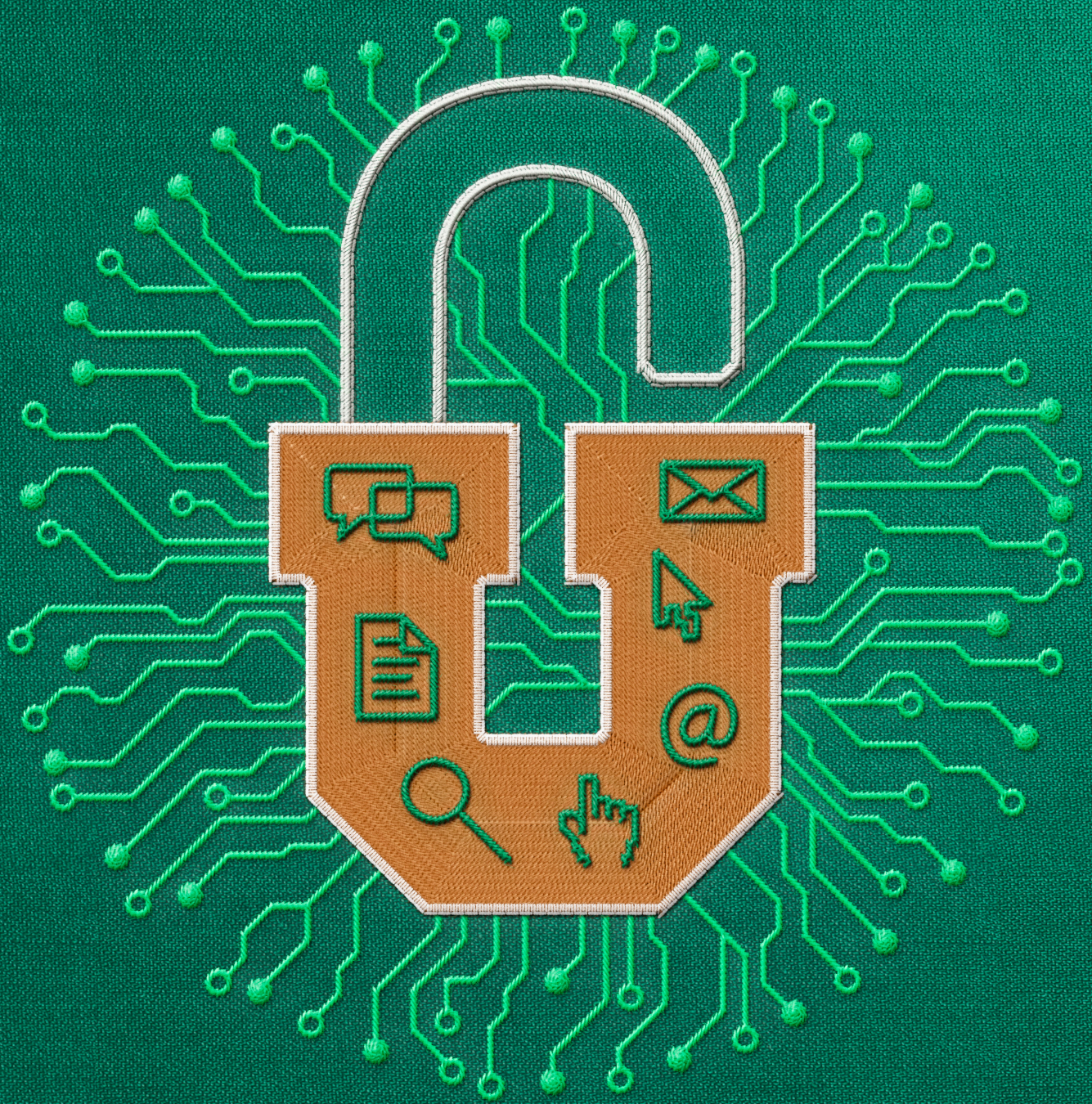
Deloitte. Insights

EDUCAUSE

A report by the Deloitte Center for Higher Education Excellence



Elevating cybersecurity on the higher education leadership agenda

Increasing executive fluency and engagement in cyber risk

ABOUT EDUCAUSE

EDUCAUSE (www.educause.edu) 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. A global nonprofit organization, EDUCAUSE members include US and international higher education institutions, corporations, not-for-profit organizations, and K-12 institutions. With a community of more than 85,000 individual participants located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. The EDUCAUSE cybersecurity program offers a number of resources to help colleges and universities develop and mature their information security and privacy programs.

ABOUT DELOITTE'S CENTER FOR HIGHER EDUCATION EXCELLENCE

Higher education institutions confront a number of challenges, from dramatic shifts in sources of funding resulting from broader structural changes in the economy to demands for greater accountability at all levels to the imperative to increase effectiveness and efficiency through the adoption of modern technology.

Deloitte's Center for Higher Education Excellence produces groundbreaking research to help colleges and universities navigate these challenges and reimagine how they can achieve excellence in every aspect of the academy: teaching, learning, and research. Through forums and immersive lab sessions, we engage the higher education community collaboratively on a transformative journey, exploring critical topics, overcoming constraints, and expanding the limits of the art of the possible.

CYBER RISK SERVICES

We help colleges and universities focus on what matters through engagements, driving alignment to institutional business risk, and balancing the need for a "frictionless" faculty and student experience. Our services work to help higher education clients:

- Guide academic and administrative leadership on risk and governance, to ensure resiliency and compliance in an ever-changing and dynamic cyber threat landscape
- Manage the explosion of digital identities and access to critical resources, both internal and cloud-based
- Secure the integrity of constituent and research data across the application ecosystem—from desktop to data center, on premise and in the cloud, utilizing standards such as NIST800-171
- Unify compliance and technology risk efforts, to apply guidance and leading practice implementation of data privacy controls
- Plan for, respond to, and recover from cyber incidents, which have the potential to significantly disrupt operations and damage reputation

CONTENTS

Introduction

With election hacking and large-scale consumer data breaches frequently in the national headlines, far less attention has been paid to an industry increasingly under attack by hackers and cybercriminals: higher education.

FROM ransomware attacks and breaches compromising the personal information of students, faculty, and staff to denial-of-service attacks that render learning-management and other systems unavailable during important times, cybersecurity threats pose an increasingly common business risk to colleges and universities.[1]

Institutions of higher education are attractive targets for two reasons. First, like health care organizations and financial institutions, colleges and universities house a wide variety of sensitive and lucrative data, including social security numbers, financial information, medical records, intellectual property, and cutting-edge research. And second, higher education's open-access culture, decentralized departmental or unit-level control, as well as federated access to data and information makes it a particularly vulnerable target for unauthorized access, unsafe Internet usage, and malware. (For more on this, see the sidebar, "What makes higher education a prime target for cybercriminals?").

This hasn't escaped the attention of the higher education information technology (IT) community. For the third year in a row, information security is the top issue identified by IT professionals on the EDUCAUSE 2018 top 10 IT issues list, and its impact on the academy has not abated.[2]

The cyber disconnect between IT professionals and institutional leaders

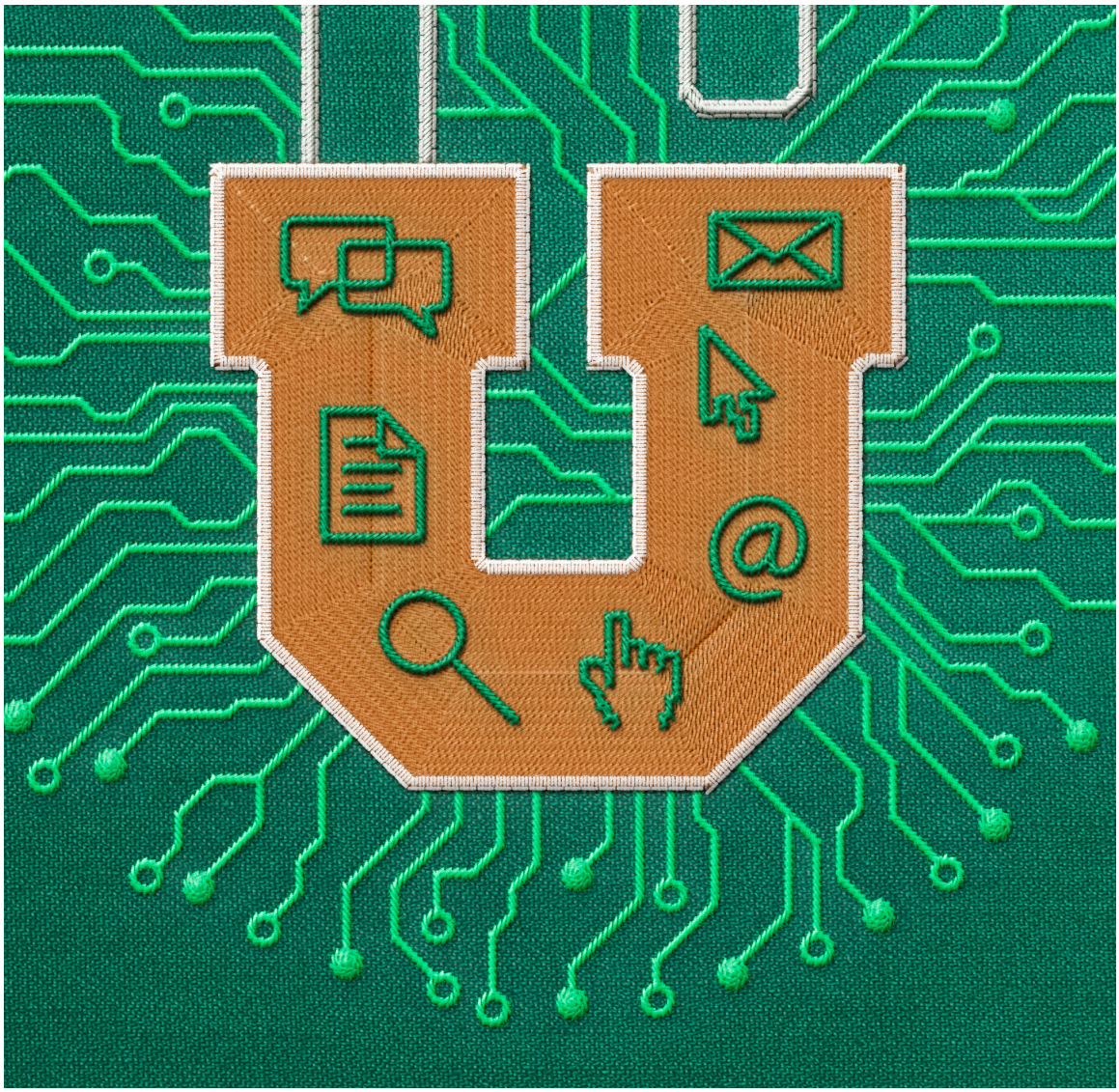
YET there remains a disconnect between IT professionals and institutional leaders. At many institutions across the country, executive engagement and board-level attention haven't yet caught up with the escalating cyber risks to which institutions are exposed. The reasons for this are threefold.

- **The traditional academic pathway to the university leadership often precludes exposure to, and experience with, cybersecurity issues:** The majority of college and university presidents and chancellors ascend to positions of institutional leadership through the ranks of academia.[3] Often this means that many college and university presidents have limited exposure to and fluency in cyber issues and their potential business impact on an institution. Boards of trustees, depending on their composition and how trustees are appointed, may or may not bring relevant experience and fluency on issues of cybersecurity to their respective institutions. Too often, it takes a major breach to escalate cybersecurity matters to the executive- and board-level agenda.
- **A president's wide-ranging scope of responsibilities leaves little bandwidth:** The demands on a president's time are many: fundraising, alumni, and donor relations, strategic planning (goal-setting and visioning), enrollment management, trustee relations, budgeting, academic affairs, community relations, federal and state relations, student life/engagement, and athletics, among others. With so many responsibilities competing for a president's time and attention, cyber discussions, which are often cast in inaccessible and technical jargon, often get sidelined by more familiar and seemingly important matters.
- **CIOs are often not members of the president's cabinet:** There's frequently a structural disconnect between an institution's highest-ranking IT official and senior leadership. Fifty-six percent of the higher education institutions surveyed by EDUCAUSE have a chief information officer (CIO) or equivalent role that is part of the president's cabinet.[4] In other words, the highest-ranking IT official has the ear of leadership at just over half of the institutions included in the survey. EDUCAUSE's higher education IT workforce study found that CIOs who serve on the cabinet are significantly more likely to discuss the IT implications of institutional decisions with campus executives.[5]

Often this means that important conversations about cybersecurity don't make it beyond an institution's IT shop to the top of the house. As Georgia State University's (GSU's) chief innovation officer Phil Ventimiglia explains, "If you really believe in cybersecurity and the importance of technology to the operation and future of the campus, then the CIO or whatever role is leading technology for the institution should be at the cabinet level."[6] It's not imperative that the CIO report to the president, but having a seat at the senior leadership table to elevate the discussion around these risks is important. For institutions where the CIO reports to an executive vice president or provost, it's important that these most senior officers regularly bring predigested, co-

gently argued, and succinctly written issues to the president and trustees.

Drawing on conversations with college and university presidents and IT leaders who have elevated cyber issues to the executive agenda, this article looks at what effective executive engagement looks like in practice and explores considerations for building a more resilient institution that's capable of bouncing back from cyber events quickly, recognizing that it's no longer a matter of if they will occur, but when.



WHAT MAKES HIGHER EDUCATION A PRIME TARGET FOR CYBERCRIMINALS?

- Wide variety of valuable data

  Institutions of higher learning have sensitive data about students, parents, alumni, faculty, and staff. Records are routinely retained decades after students have graduated from an institution. Furthermore, colleges and universities, particularly those that engage in high volumes of research, often house proprietary data from a wide range of corporations and government entities. Moreover, institutions with ties to local and regional hospitals generally store confidential medical data. In short, the sheer volume of potentially valuable data housed at most institutions of higher learning tends to make them highly attractive targets.

- Lack of centralized structure

  Institutions tend to house their sensitive data in many different locations rather than one centralized hub. Student data may be kept separately at each college within a university or at different branches in a statewide university system. The same data may be kept in a variety of other locations, as well: alumni offices, central administration, or even at the department level for graduate programs. Sensitive data relating to corporate or government grants may be housed in the departments that receive those grants or even on the devices of individual professors and graduate students who play key research roles. This decentralized structure can give cybercriminals a wide range of paths to exploit vulnerabilities in the disparate systems that house sensitive data.

- Organizational vulnerabilities

  The decentralized nature of data storage in institutions of higher education is often paralleled by similar organizational and structural issues. The responsibility for implementing security measures and determining processes may lie with a number of different stakeholders in a wide range of departments. Institutions generally lack a top-down command structure that makes new safeguards easy to implement; so departments, individual professors, or students may be slow to engage in the practices necessary to improve security.

- Widespread use of personal devices

  Administrators, faculty, and staff are often unaware of the extent to which they may be exposing their institution to cyber risks when they download sensitive data to less well-protected personal devices. At last count, 93 percent of faculty reported owning a smartphone, while just 27 percent received mandatory information security training.[7] As a result, even if an institution has robust security measures in place, any number of individuals at the institution may, through carelessness or unintentionally, through lack of awareness, expose sensitive data.

Routine exposure: Ensuring structural alignment

CIOs who are cabinet members are generally in a better position to raise strategic IT issues, including cybersecurity risks to the institution, presidents, and boards of trustees.

By virtue of this structural alignment, institutional leaders tend to have greater exposure to an issue set that may otherwise be confined to the technology shop. The direct reporting relationship to the president often serves as "a way of keeping the lines of communication open, so that when we have situations like a distributed denial of service attack or something that's highly disruptive, I don't have to build the foundation. It's already in place and it's just a matter of zeroing in on a particular direction," says Rutgers University's senior vice president and CIO Michele Norin.

As GSU president Mark Becker explains, "The chief information officer (or equivalent) has to be at a high level in the organization; they can't be buried away from the president. At Georgia State, they report directly to me and sit on my cabinet, as well as on the administrative council [which allows us] to have direct conversations. Our offices are on the same floor."[8] This kind of routine exposure and access typically facilitates greater understanding of the cybersecurity issues facing the institution.

For American University (AU), the elevation of the CIO role to the vice president level and appointment to the president's cabinet began with the recognition that the CIO is an institutional actor and therefore required to understand all the major features of the institution. As AU president emeritus Neil Kerwin recounts, "With a seat on the cabinet, the vice president of information technology educates colleagues on the senior management team and is educated by them. That works its way ultimately up to the board of trustees, which now has a fixed expectation of IT being an agenda item for every board meeting." Dave Swartz, AU's vice president and CIO observes, "At most universities, what CIOs struggle with is having the authority to be able to put in place the controls that are needed to be sure that risks are mitigated." The result of AU's change in organizational structure was "better alignment between responsibility and authority and accountability."

Right framing: The lingua franca for communicating cyber risk

Too often, overly technical and esoteric cyber-speak obscures the bigger picture issues of concern for institutional leaders. To gain traction with presidents and boards of trustees, the conversation around cybersecurity should be reframed in terms of enterprise risk management, with the business impact to the institution clearly spelled out. As GSU president Mark Becker puts it, "What I want to know is where our greatest vulnerabilities are and what are we doing to minimize those in a cost-efficient manner."

GSU has gone so far as to put in place a cybersecurity charter to communicate to the institution writ large that cybersecurity is not an IT domain but rather an enterprise risk. "In today's world, where information storage and processes like monetary transactions are increasingly carried out digitally, we all see instances in the news where unauthorized data access has put large numbers of people's personal information at risk. As a large organization, we are stewards of a variety of sensitive data, so solid information security practices are vital to protecting our students, faculty, and staff, as well as all those who conduct business and research in partnership with the university," explains Ren Flot, GSU's chief information security officer and director of cybersecurity services.

The business risks associated with a breach can range from financial and reputational impact to the ability of an institution to carry out its mission.

- **Financial impact:** The sheer financial cost of a breach can be significant. Research at the Ponemon Institute suggests that when factoring in all the different costs (including customer loss, the time to detect a breach, the costs of fixing identified vulnerabilities, the costs of compensating victims, public relations, and so on), the average data breach cost institutions of higher learning about $260 per record seized in the incidents they analyzed over the past four years.[9]
- **Impact on operations:** Because virtually every facet of the modern university depends to some extent on properly functioning technology, a significant data breach can be crippling to the daily operations of a university. For example, a large-scale breach at one major university recently prevented students from being able to access their learning management system for several hours during finals week. As AU president emeritus Neil Kerwin points out, "The kind of damage a breach can cause at a university is not confined to access to information in a narrow sense but literally affects the ability of the institution to conduct its mission."

  As the reliance on technology at institutions of higher learning grows year over year, the magnitude of potential disruptions to daily business operations will likely only increase. As GSU's Mark Becker observes, "The future in higher education is how to leverage technology to deliver a better education at a lower cost. The integration of the technology is going to happen. We have to do that in a secure environment."
- **Reputational damage with consumers, corporate partners, and government agencies:** Corporations are less likely to be interested in partnerships with universities whose research data has been breached or with institutions that seem to lack a clear, strong resilience plan and set of processes for dealing with cyber threats. In addition to the concerns they share with corporations, universities often need to comply with strict regulatory considerations (such as NIST 800-177) for government grants and contracts.

Finally, if important student, parent, or alumni data is seized in a breach, the university's reputation with potential enrollees may suffer, especially if a robust response plan with a strong public relations element is not in place.

Resilience mind-set: It's no longer a matter of if, but when

YESTERDAY'S relatively isolated malicious activity has given way to well-organized cybercrime enterprises and networks of politically motivated, and sometimes state-sponsored, attackers. Verizon's *2017 data breach investigations* report found that state-affiliated actors and organized criminal groups were behind an increasing number of breaches targeting the education sector.[10] Against this backdrop, it seems inevitable that some cyber incidents may occur.

While an institution's technical team handles many day-to-day, routine security events, some incidents may become more serious business crises that can affect an institution's broader mission. In more serious events, it is imperative that the business closely collaborates with IT to maintain effective resiliency. As GSU's Ventimiglia observes, "We're in a day and age that if a network goes down for an hour, you can't teach."[11]

Being resilient means having the capacity to rapidly contain the damage and mobilize the diverse resources needed to reduce impact—including direct costs and operational disruption, as well as damage to reputation.

Effectively developing this capability generally requires executive- and board-level engagement.

Every institution should realistically assess its changing risk profile and determine what levels and types of cyber risk they consider acceptable. Just three-quarters of higher education institutions surveyed by EDUCAUSE have conducted any sort of security risk assessment.[12] This is a business challenge, not just a technical one. Presidents and trustees need enough understanding of the threat landscape to provide cyber risk guidance. It's then the job of the technical team to translate this into effective operational capabilities.

While resilience requires investment in traditional technology-based redundancy and disaster recovery capabilities, the bigger picture includes a complete set of crisis management capabilities. It involves IT, as well as leaders across the institution, and decision-makers from legal, risk, human relations, and communications functions. It typically requires a playbook across all these entities, designed in advance by considering how threat scenarios impacting critical assets and processes could play out.

Beyond playbooks, developing a robust resilience capability can be supported through cyber wargaming and simulations. Staging simulations can create better organizational awareness and understanding of threats, improve cyber judgment, and facilitate the development of "muscle memory" that helps teams respond flexibly and instinctively to both the simulation scenarios, as well as situations that cannot be foreseen.

Many higher education institutions apply a different philosophy to wargaming and security. As Virginia Tech's information technology security officer Randy Marchany explains, "This is the difference between a 'keep them out' versus 'we assume they're in' approach. This viewpoint changes how institutions respond to a wargame scenario. If it is assumed that attackers are already in the system, it's a matter of 'how do I hunt them down' as opposed to 'how do I keep them out.'"

Users are inevitably going to make mistakes. The question is how to reduce the damage once a mistake is made. For its part, GSU is using outside companies to monitor the traffic into and out of the university 24/7. The university is also virtualizing its entire network, which will enable it to see any rogue activity in the network and isolate the source and quickly reduce the risk.

Looking ahead

UNTIL recently, it has frequently taken a major cyber incident to elevate cybersecurity to the executive agenda. But with the increasing digitization of the academic enterprise, growing regulatory pressure to improve an institution's information security posture, and a fast-evolving cyber threat landscape, the stakes are higher than ever for institutions that don't treat cybersecurity matters as serious enterprise risks with the attendant executive- and board-level attention they warrant.

Increasing executive- and board-level fluency in cyber issues is part and parcel of responsibly overseeing and governing an institution, given the reality of today's growing cyber threats. Developing such fluency often requires getting the structural alignment in place (to the extent it's not already there), reframing the issue as one of enterprise risk management, and developing institutional resiliency so that colleges and universities are in a position to bounce back quickly if an incident occurs.

RECOMMENDED READING

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. The EDUCAUSE Cybersecurity Program offers a number of resources to help colleges and universities develop and mature their information security and privacy programs. Recommended readings pertaining to the topic of this report include:

- EDUCAUSE featured topic guide, *Developing a risk-based security strategy in higher education*, January 2018. Plan for, respond to, and recover from cyber incidents, which have the potential to significantly disrupt operations and damage reputation
- EDUCAUSE, *Digital capabilities in higher education 2016, information security report*, November 2017.
- EDUCAUSE, *Information Security Program Assessment Tool*, last updated September 2017.
- Emily Mossburg, John Gelinne, and Hector Calzada, "*Beneath the surface of a cyberattack: A deeper look at business impacts*," Deloitte, 2016.

ENDNOTES

1. According to Verizon's 2017 *data breach investigations report*, 455 cybersecurity incidents occurred in the education sector in 2016, 73 of which resulted in data disclosure.
2. EDUCAUSE, "Top 10 IT issues, technologies, and trends," accessed February 12, 2018.
3. Jeffrey Selingo, Sonny Chheng, and Cole Clark, *Pathways to the university presidency: The future of higher education leadership*, a report by Deloitte's Center for Higher Education Excellence in conjunction with Georgia Tech's Center for 21st Century Universities, Deloitte University Press, April 18, 2017.
4. EDUCAUSE, "2017 EDUCAUSE core data service," accessed February 12, 2018.
5. Jeffrey Pomerantz and D. Christopher Brooks, *The higher education IT workforce landscape, 2016*, EDUCAUSE Center for Analysis and Research, April 2016.
6. Mark Becker and Phil Ventimiglia, joint interview.
7. EDUCAUSE, "The EDUCAUSE almanac for faculty and technology survey, 2017," accessed February 12, 2018.
8. EDUCAUSE Annual Conference 2017, "The importance of cybersecurity governance: Perspectives from presidents, trustees, and IT leaders," November 3, 2017.
9. IBM Security and Ponemon Institute, *2017 cost of data breach study: United States*, June 13, 2017.
10. Verizon, *2017 data breach investigations report: 10th edition*, accessed January 29, 2018.
11. EDUCAUSE Annual Conference 2017, "The importance of cybersecurity governance," November 3, 2017.
12. EDUCAUSE, "The EDUCAUSE core data service almanac."

ABOUT THE AUTHORS

TIFFANY DOVEY FISHMAN

Tiffany is a senior manager with the Deloitte Center for Government Insights. Her research and client work focuses on how emerging issues in technology, business, and society will impact organizations. She has written extensively on a wide range of public policy and management issues, from health and human services reform to the future of transportation and the transformation of higher education. Her work has appeared in a number of publications, including Public CIO, Governing, and EducationWeek.

COLE CLARK

Cole leads client and community outreach and relationships for Deloitte Services LP's Higher Education practice. He has more than 25 years global experience in education technology and six years of global higher education business application leadership at Oracle Corporation across the major functional areas of the academic enterprise, including student lifecycle, HR, and finance. Cole has been a trusted advisor in the higher education community and a leading voice around transformation, using modern technologies as enablers underneath broader strategies to increase efficiency and effectiveness. In addition to the core business functions of the institution, Cole has experience in areas of the "front office" of higher education including research administration, student engagement, recruitment and retention, and student success.

JOANNA LYN GRAMA

Joanna Lyn Grama directs the EDUCAUSE Cybersecurity Initiative and the IT GRC (governance, risk, and compliance) program. She is a member of the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee and serves as the chair of its technology subcommittee.

ACKNOWLEDGEMENTS

In summer 2017, Deloitte and EDUCAUSE convened a panel to discuss cybersecurity issues in higher education. Deloitte and EDUCAUSE extend their thanks to the following working group members:

Ahmed El-Haggen, vice president for information technology & CIO, Coppin State University

Patrick Feehan, information security & privacy director, Montgomery College

Cathy Hubbs, chief information security officer, American University

Randy Marchany, information technology security officer, Virginia Tech

Ed Martin, deputy chief information officer, George Washington University

Scott Midkiff, vice president for information technology & CIO, Virginia Tech

Deloitte and EDUCAUSE also wish to extend their thanks to the following higher education leaders who were interviewed as a part of this project:

Mark P. Becker, president, Georgia State University

Michael Gower, executive vice president for finance & administration, Rutgers, The State University of New Jersey

Cornelius M. Kerwin, president emeritus, American University

Michele Norin, senior vice president and chief information officer, Rutgers, The State University of New Jersey

Timothy D. Sands, president, Virginia Tech

David Swartz, vice president and chief information officer, American University

Phil Ventimiglia, chief innovation officer, George State University

This project would not have been possible without the leadership of **Dave Noone**. Thanks also go to **Susan Grajek, Valerie Vogel, Karen Wetzel, Richard Rudnicki, Allison Eng-Perez, Betty Fleurimond, Justin Williams, Michael Wyatt,** and **John Curry.**

CONTACTS

Mark Ford
Sector leader, Higher Education
Deloitte Risk and Financial Advisory
Principal
Deloitte and Touche LLP
+1 313 394 5313
mford@deloitte.com

Betty Fleurimond
Managing director, Higher Education
Deloitte Services LP
+1 202 492 1453
bfleurimond@deloitte.com

Richard Rudnicki
Specialist leader
Deloitte & Touche LLP
+1 313 401 5263
rrudnicki@deloitte.com

Justin Williams
Senior manager
Deloitte & Touche LLP
+1 346 224 5001
jmwilliams@deloitte.com

Joanna Lyn Grama
Director of cybersecurity and IT GRC programs
EDUCAUSE
+1 720 406 6769
jgrama@educause.edu

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Ramani Moses, Abrar Khan, Preetha Devan
Creative: Anoop K R, Emily Koteff Moreano
Promotion: Shraddha Sachdev
Artwork: Alex Nabaum

About Deloitte Insights
Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.