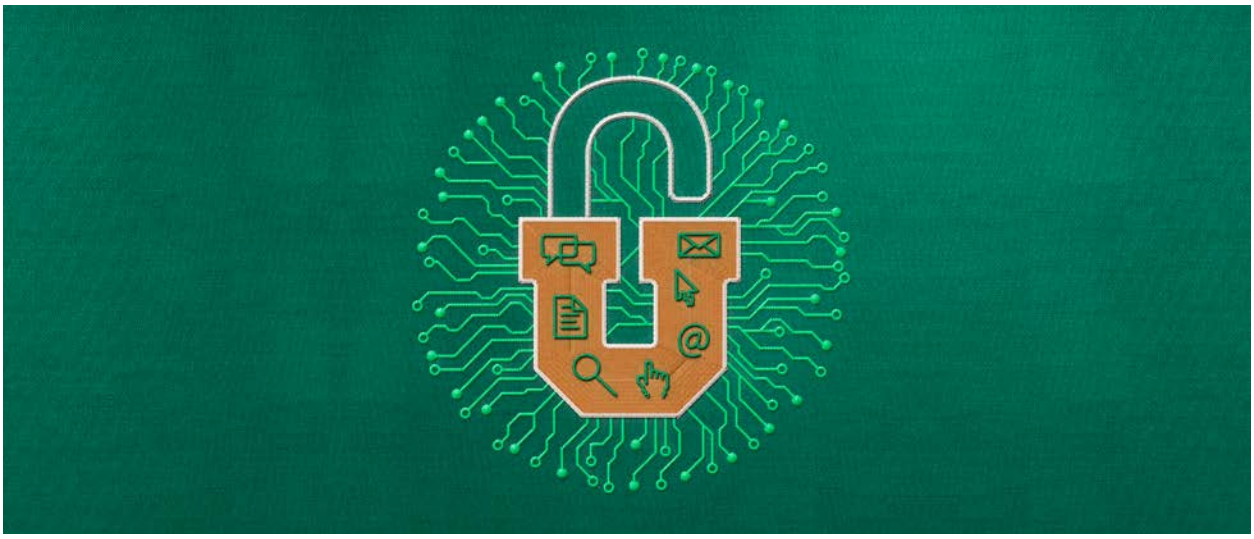


Elevating cybersecurity on the higher education leadership agenda

Increasing executive fluency and engagement in cyber risk

By Tiffany Dovey Fishman, Cole Clark, and Joanna Lyn Grama

What's the story?

Institutions of higher education are attractive targets of cybersecurity threats for two reasons: First, 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.

This hasn't escaped the attention of the higher education information technology (IT) community. Yet there remains a disconnect between IT professionals and institutional leaders. How can higher education institutions bridge this gap and build robust cybersecurity into university IT systems?

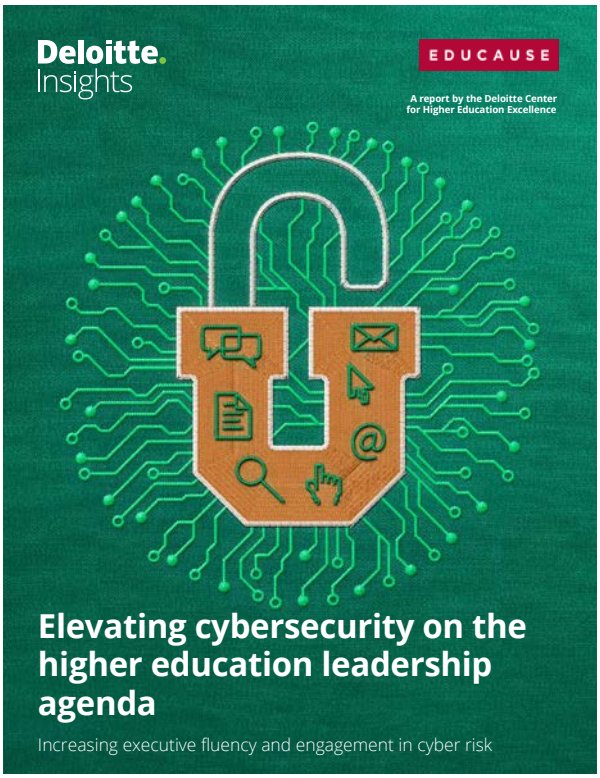
Who at my client is impacted?

- **Sector:** Higher education institutions – colleges and universities
- **Roles:** C-Suite executives, business leaders, and managers in higher education institutions and cybersecurity, CIOs, and CISOs

What issues does this address?

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.

- **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.
- **Right framing: Lingua franca for communicating cyber risk to institutional leaders**. Overly technical and esoteric cyberspace 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.



- **Resilience mindset: It's no longer a matter of if, but when**. 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.

What do I do now?


Read the full Deloitte Review article **here**


Explore the entire **Public Sector** collection


Email a copy of the report to clients/targets


Contact the authors to arrange one-on-one client meetings/briefings on the topic


Print a copy of the article to give to your clients


Post the article to your social networks on LinkedIn, Twitter, and Facebook

Who can tell me more?

For more information, and to discuss how this article may be relevant to your client, contact:

- **Tiffany Dovey Fishman**, subject matter specialist, Deloitte Services LP
- **Cole Clark**, lead, Deloitte Services LP's Higher Education Practice
- **Joanna Lyn Grama**, director, Cybersecurity and IT GRC Programs, EDUCAUSE
- **Amy Bergstrom**, senior manager, Deloitte Insights