SailPoint

WHITE PAPER

The Effects of Underutilizing **Identity in Higher Education**

Executive Summary

Higher education is a prime target of cyberattacks as institutions typically house and manage Personally Identifiable Information (PII) and Protected Health Information (PHI). Moreover, colleges and universities often possess sensitive research material. In some cases, they may even be collaborating with the Department of Defense (DoD) on projects containing classified content.

While keeping such sensitive information secure from hackers and cyber-criminals is critical, educational institutions must be equally vigilant in mitigating insider risk. Anyone with authorized access to applications and data files can trigger a data breach whether by intent or negligence. As a result, the higher education industry has become the third most likely source of data breach, trailing behind only the healthcare and financial sectors.

For these reasons, security has become a top concern for IT professionals in the education space. But unlike other industries, higher education must juxtapose this priority with maintaining an open, collaborative culture and providing the best experience possible for users accessing applications and files. Unfortunately, we find in this research, higher education is falling short on all three fronts.

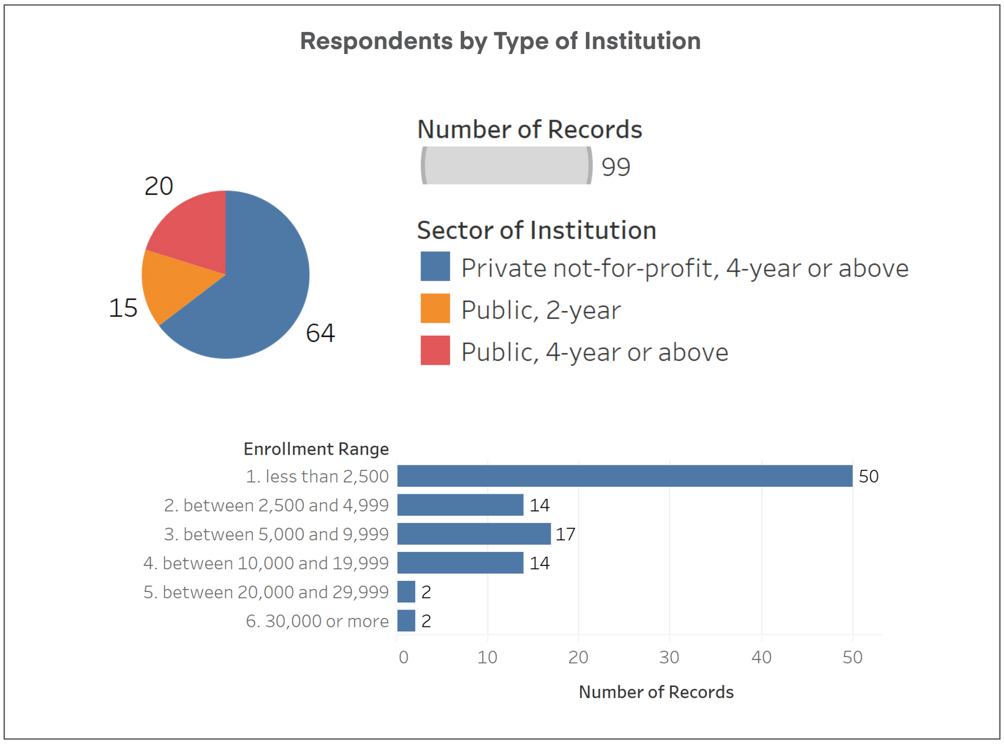
In this study, we look at why educational institutions continue to struggle with achieving the critical balance of delivering timely access while protecting sensitive data to a large, dynamic and extremely diverse user population. Furthermore, we will explore the role that identity governance should play in delivering security while enhancing user access to information.

Methodology

For this research, the Tambellini Group provided summary data obtained from a survey conducted in August 2018. A total of 99 qualified respondents completed the survey. The institutions included in this research range in sector (private and public) and size based on student enrollment.

All respondents were decision makers. More specifically, 92% were either Chief Information, Technology or Risk Management Officers.

Figures A and B



Source: The Tambellini Group Education Institution Technology Profile Database®

Understanding Identity Governance

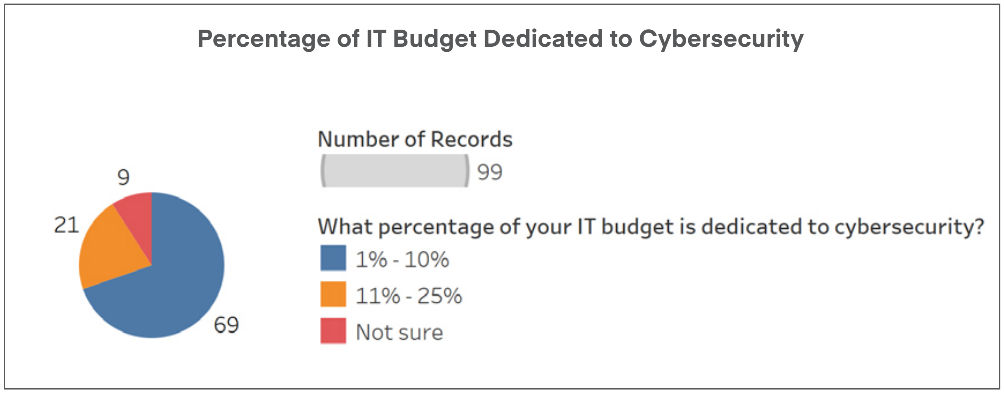
Identity governance enables and secures digital identities for all users, applications and data. It achieves this by helping institutions identify who currently has access, who should have access, and how access is being used. Ultimately, identity governance improves security, privacy and compliance by defining and enforcing access policies. Furthermore, it drives efficient IT operations and enhances the user experience through self-service capabilities such as password reset and access requests as well as automated provisioning.

Study Findings

1. Resource Allocations Appear Misaligned with Cybersecurity Needs and Concerns

In 2018, Educause reported that higher education leaders ranked information security their top concern for the third consecutive year. Moreover, EdTech recently published data indicating the number of breaches within the education sector more than doubled between the second half of 2016 and first half of 2017. A total of 118 successful attacks on educational institutions during the first half of 2017 accounted for 13% of all reported breaches, with only financial and healthcare sectors experiencing more.[1] These numbers are alarming. Yet in this latest study, the Tambellini Group found most respondents allocating no more than 1/10th of their IT budget for cybersecurity. *(Figure 1)* This indicates potential misalignment between expressed concerns rising from ongoing data breaches and the amount of resources allocated to mitigating risk.

Figure 1



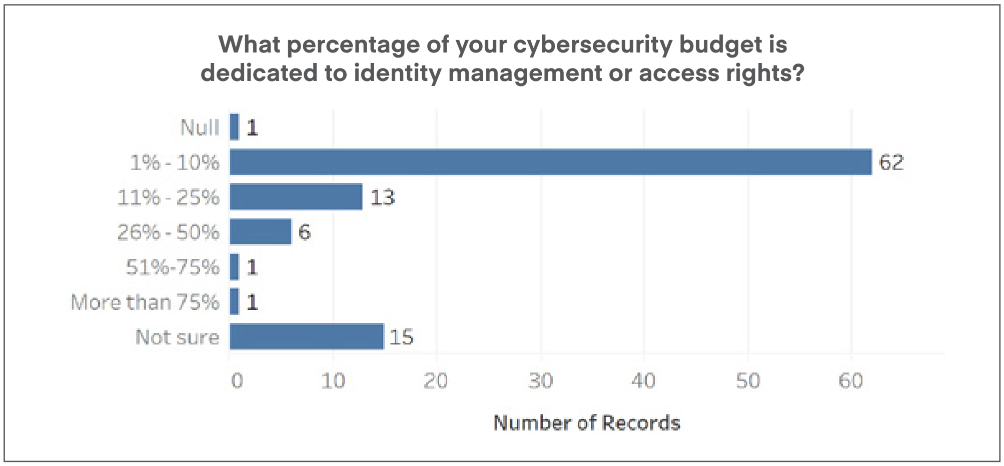
Source: The Tambellini Group Education Institution Technology Profile Database®

One way to effectively mitigate risk around security, privacy and compliance is by properly governing digital identities and their access entitlements. If institutions can see and manage who accesses what, when and how, they can reduce the attack surface. In fact, Gartner analysts have suggested that *“by 2021, organizations with complementary/integrated (identity governance capabilities across applications and files) will suffer 60% fewer data breaches”*[2]

Despite this counsel, most respondents in this survey are currently spending no more than 1/10th of their cybersecurity budget on identity technology – indicating another potential misalignment between resource allocation and needs. (*Figure 2)*

[1] Meghan Bogardus Cortex, *Education Sector Data Breaches Skyrocket in 2017*, EdTech, Dec. 2017
[2] Brian Iverson and Marc-Antoine Meunier, *Prepare for Consolidation of How Access Risk Is Managed Across Infrastructure, Applications and Data*, Gartner, Nov. 2017

Figure 2

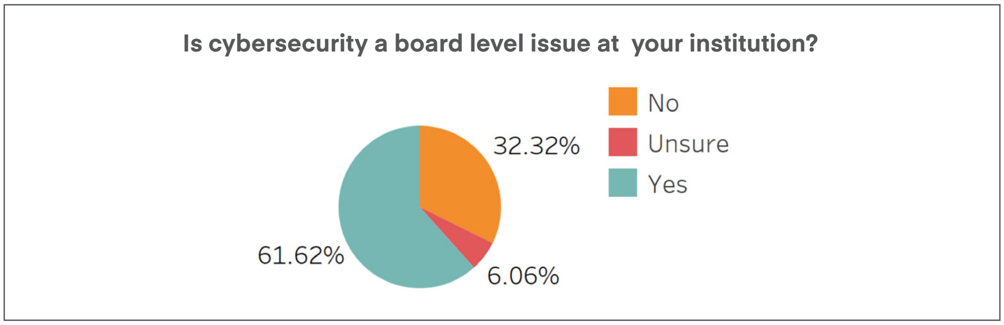


Source: The Tambellini Group Education Institution Technology Profile Database®

2. Low Engagement from Senior Management and Board Members

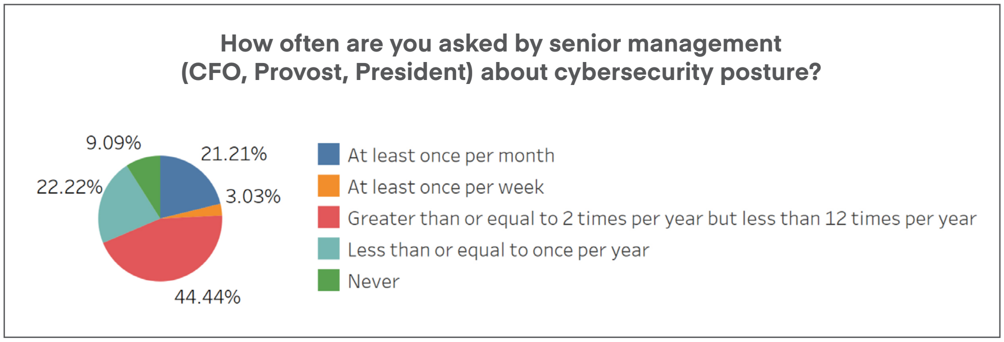
Figure 3 indicates 38% of board members lack visibility into cybersecurity efforts and nearly 30% *(Figure 4)* of senior executives fail to inquire about their institution's security posture even once a year. These numbers are alarming given the consequential nature of being unaware or unengaged in cybersecurity.

Figure 3



Source: The Tambellini Group Education Institution Technology Profile Database®

Figure 4



Source: The Tambellini Group Education Institution Technology Profile Database®

3. Identity Recognized as Cybersecurity Function but Remains Underutilized

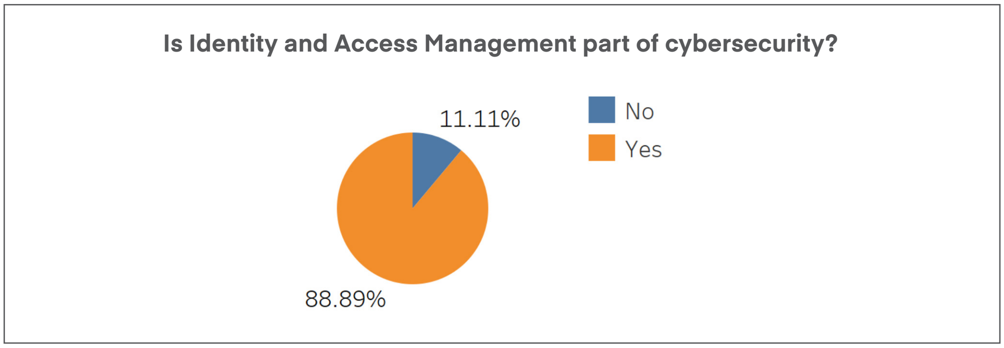
While the market exhibits a diverse set of solutions to address the spectrum of cybersecurity threats facing educational institutions, identity governance is central to any effective cybersecurity program.

One reason for this is because hackers often target users to gain access to high-value systems and data.

Considering the sheer volume of digital identities accessing the myriad of applications and data files, colleges and universities could have millions of access points that translate into points of exposure.

Identity governance mitigates this risk by enabling institutions to see and govern the access rights of all digital identities. While Figure 5 indicates that 88% of the respondents in the Tambellini research recognize the power of identity, the application of the technology by educational institutions appears rudimentary. Figure 6 provides evidence of this assertion.

Figure 5



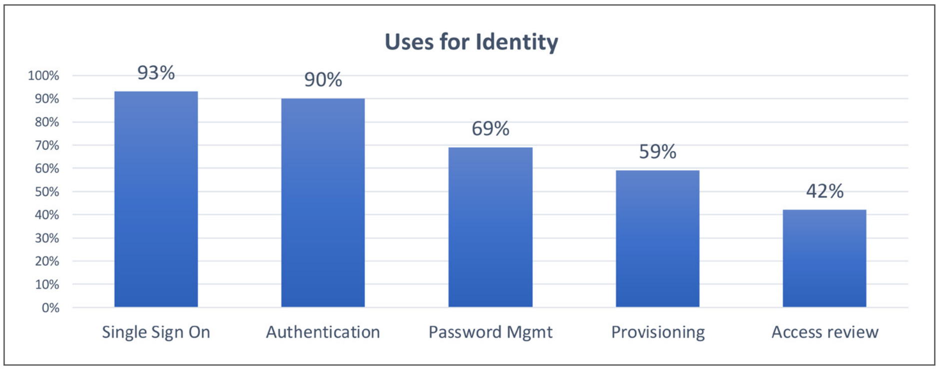
Source: The Tambellini Group Education Institution Technology Profile Database®

4. Identity is Not Being Used to its Full Extent

In Figure 6, we learn how educational institutions are applying identity technology. Most respondents are leveraging identity for single-sign-on and authentication. The numbers drop dramatically from 90th percentile to 69 as it relates to password management. Use of identity for provisioning and access reviews decreases even further to 59 and 42 respectively. Within these few data points, we gain deep insight into the operational and security gaps facing higher education.

First, password management enables users to change or reset passwords while enforcing strong policies across all applications and user populations. By enabling end users to perform password reset and change requests themselves, you can significantly reduce the burden on your help desk staff while improving the enforcement of strong security policies. Yet the Tambellini study indicates that 1/3rd are not exploiting this capability to drive efficiency and security. This directly impacts user experience, drives up costs, and increases security risk.

Figure 6



Source: The Tambellini Group Education Institution Technology Profile Database®

Second, provisioning under a unified and consistent governance policy allows institutions to avoid improper or inconsistent provisioning and de-provisioning. It further reduces delayed access for users and softens the workload for IT administrators and data stewards. For these reasons, it is highly alarming that 4 in 10 respondents from this survey indicated they were not utilizing an identity governance platform to consistently provision users. While these respondents were not asked how they were provisioning, we can draw from general knowledge and anecdotal experience. Many are provisioning via the functionality native to each individual application. In fact, we often find institutions using archaic processes that simply diminish user experience and create security gaps. For instance, some colleges and universities provision access by creating a ticket through ServiceNow. That ticket is then forwarded to admins who manually grant access to individual users. This is highly inefficient and not scalable by any means. If educational institutions want to protect data, maintain an open and collaborative culture and improve user experience, they must centralize and automate critical processes. These processes include determining whether a user should be granted access, and then provisioning. Applying such automation through identity governance technology can dramatically increase efficiency and deliver secure and timely access.

Third, access certifications are critical in environments where the user population is dynamic and transient. Reviewing entitlement rights regularly ensures that only the right people have the right access at the right time. Moreover, it provides the documentation to meet corporate and regulatory compliance. Identity governance enables educational institutions to automate the process of reviewing user access rights. It can initiate campaigns for business managers to approve or revoke access as part of a centralized governance program. That said, the research indicates that only 42% of survey respondents are using their identity platform for access reviews.

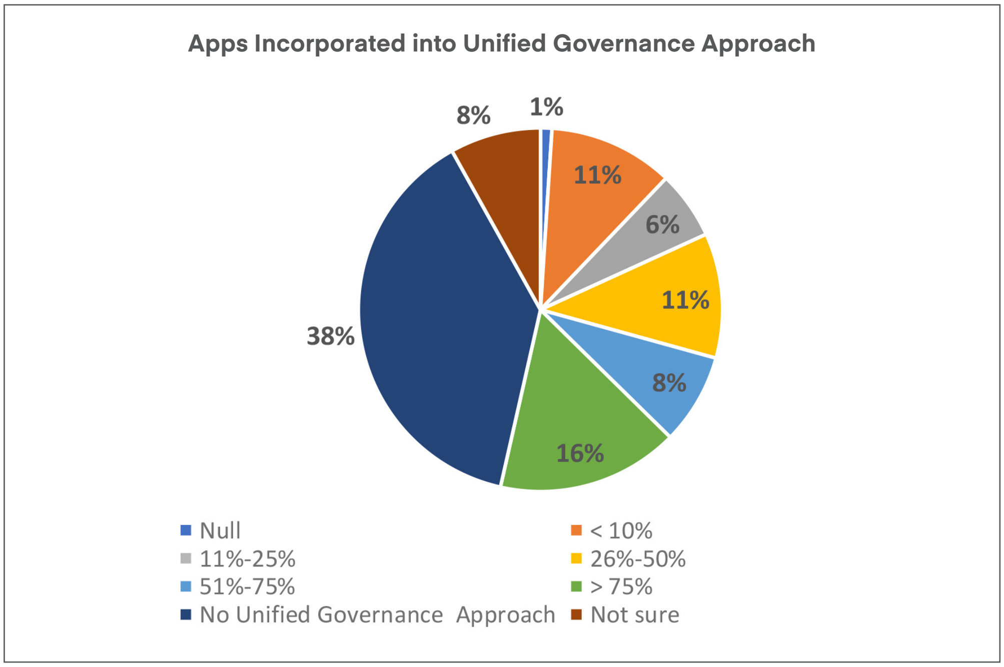
5. Institutions Leaving Security Gaps

Disparate processes for managing user access to various applications can result in security and compliance gaps. For this reason, educational institutions should incorporate as many applications as possible into a unified governance approach. However, the Tambellini Group survey suggests that 3 out of 4 colleges and universities have incorporated fewer than half of their applications into their identity governance platform. Nearly half (46%) either have zero applications incorporated or do not know if they have any rolled into identity governance. *(Figure 7)*

Given that colleges and universities are continuously on-boarding and operating numerous applications, it is imperative that these critical gaps are addressed to protect sensitive information stored in systems, applications, and file storage folders. Doing so allows institutions to:

- Align policy and centralize access controls across the institution
- Automatically grant and revoke access based on training criteria
- Eliminate stale entitlements through automatic certification campaigns
- Give managers visibility into what access their direct reports have
- Detect, document and alert appropriate security teams regarding any attempts to circumvent governance processes

Figure 7



Source: The Tambellini Group Education Institution Technology Profile Database®

Conclusions

While cybersecurity within higher education has risen to the top of IT concerns, efforts to counter threats remain immature. Not only is there room for improvement to drive awareness and engagement from senior management and board members, but there is also a technology gap to fill. Even when comprehensive identity governance is available to mitigate cybersecurity and compliance risks, the application of this technology by many institutions appears embryonic. Educational institutions seeking to address risk while preserving an open, collaborative culture need to consider fully adopting a comprehensive, intelligent identity solution as a critical foundation for governing and protecting user information residing in cloud or on-premises applications and data files.