Getting schooled

Identity and access managment

To strengthen their cybersecurity perimeter, colleges and universities may need a crash course in enhancing the management of user access to their networks.

kpmg.com

Introduction

Each fall, tens of thousands of young people begin their studies at colleges and universities around the country. In years past, these incoming students would receive a freshman handbook to get them started on their college careers. Today, they get an e-mail asking them to create their username and password to gain access to the school's network. With that, they can register for classes, pick a roommate, network with their peers—and allow mom and dad to pay the tuition bill.

Like most enterprises, colleges and universities rely on their internal computer networks to operate effectively. But when it comes to managing access to their systems, schools face a number of unique challenges. In addition to the influx of freshmen in the fall, the spring sees a similar number of seniors leave their alma maters for graduate school or the world of work. Faculty often have multiple roles requiring separate access levels. Visiting professors need access to the school's network for a time but should be blocked once they leave. And the growing popularity of mobile devices and cloud-based applications present their own issues.

Keeping track of all these different and changing network users opens up a significant cybersecurity challenge for colleges and universities—the risk of identity theft being used by hackers to gain access to the school's networks.

Colleges and universities present rich targets for cyber criminals, so that risk is very real. Students and parents provide schools with significant amounts of private, personal, and financial information. In addition, larger institutions, often in partnership with private enterprises, engage in proprietary research that would be of interest to competitors or even foreign governments.

While identity theft has predominantly affected the financial services and retail industries, the threat is spreading to other sectors, including healthcare and now to education. A number of high-profile schools have fallen victim to black-hat hackers. Such hacks can result in financial damages and tarnished reputations. In addition, exposure of personally identifiable information (PII) or financial information can have legal and regulatory ramifications.

In many of these cases, the typical way in has been through a stolen identity. To protect themselves, schools must be proactive to uncover where the greatest identity risks reside and consequently which individuals and accounts need to be watched. To do so, schools need to have a thorough understanding of user identity and levels of access, so they can begin to uncover malicious or anomalous behavior before it becomes a problem.

One way colleges and universities can better protect themselves from cyber attacks is to implement a comprehensive program for IAM that can be applied to all staff, faculty, and students, as well as other relevant parties, such as alumni. IAM is a set of processes and technologies that facilitate creating, maintaining and using a single digital identity. By applying the processes, controls, and technologies around IAM, schools can help limit cyber attacks by building a more secure perimeter around their networks.

Why hackers like to go to college

Hackers are increasingly eyeing colleges and universities as targets for their cyber attacks. In 2015, 550 universities reported some kind of data breach, according to Symantec's Internet Security Threat Report. In one of them, the University of California (Berkeley) had to notify about 80,000 current and former faculty, staff, students, and vendors following a criminal cyber attack on a system storing personal and financial information.[1]

What makes colleges and universities so enticing for cyber criminals? Consider that in one breach, hackers can have access to thousands of IDs, Social Security numbers, bank accounts, credit cards, and health information from students and their parents.[2] Hackers may also be able to find other personal and biographical information that can offer clues that could enable them to break into other types of accounts held by the students and their families.

Many colleges and universities work on large research projects for the government or private sector, offering another rich target. Hackers wanting to gain access to these projects would include business competitors seeking intellectual property and even state actors that may be looking for national security information.

Given the amount and sensitivity of all this information, security breaches at colleges and universities can have significant consequences. Schools can suffer reputational damage from bad publicity and the possibility of personal or embarrassing information being made public. Consider the fallout if a school known for its IT curriculum falls victim to a cyber attack.

Breaches can be costly as well. According to the Ponemon Institute, the education sector has one of the highest per capita data breach costs at $259 for each record containing sensitive data. The University of Calgary in Canada learned how costly an attack can be after hackers created encrypted copies of files a student stored in a Dropbox account and demanded a ransom to open them. The school was able to retrieve the data from backup systems, but the university did pay the ransom of US$15,000 as a precaution.[3] In addition to buying off hackers, schools may have to pay restitution or fines. And leaked research can expose proprietary information, leading to financial loss and the potential withdrawal of grants and contracts.

[1] Campus alerting 80,000 individuals to cyberattack. Janet Gilmore. *Berkeley News.* February 26, 2016

[2] Cyberattack 101: Why Hackers Are Going after Universities. *NBC News Tech* September 20, 2015

[3] 'Ransomware' cyberattack highlights vulnerability of universities. *Brian Owens.* June 17, 2016. www.nature.com

How hackers get in

The common denominator around many cyber attacks is a failure to enforce controls around the identity layer. In these cases, the cybercriminal acquires the log-in credentials of a person who has access to a network. But gaining access to the network is only the first step. Hackers want to infiltrate the highest levels of privilege in a network to put themselves in reach of the most sensitive and useful information. So they may start with a lower-level user, then look for accounts with greater access levels to provide entry to databases, root access to services, or access to network firewalls and routers.

Often, hackers uncover user credentials through a ruse or other surreptitious ways. For example, the practice of phishing uses a convincing e-mail to trick the victim into clicking on a link that will reveal information, such as a password. Recently, Augusta University fell victim to a phishing scam and had to instruct its employees and students to change their passwords.[4]

Other times, identities can be stolen because of lax policy or the failure of individuals to follow cyber security measures.

We have already seen how the misuse of Dropbox led to hacking at The University of Calgary. Because they are easy to use and readily available, these external storage services can be a great temptation for faculty and students if the school's network is not easily accessible.

Another practice of vulnerability is sometimes called the "phone a friend" scenario. For example, a new staff member joins a university's research team. His supervisor contacts a friend in IT and asks for a certain level of network access for the new hire. This practice can be repeated throughout this employee's career, leading to risky situations, like a lack of segregation of duties, where an individual can request and approve a purchase, for example. Moreover, the phone-a-friend scenario leaves no records and offers no accountability. So if the staffer leaves, his or her online identity is likely to remain and become a potential way in for hackers. A similar situation can occur when students are assigned to a research project for a semester and then move on at the end of the term.

Another way colleges and universities become more vulnerable to identity theft is by changing or granting network access to a large group of users en masse, such as converting all graduating seniors to alumni-level access. Anything done to a large number of accounts is likely to create problems for maintaining identity security because it provides access indiscriminately, that is, without confirming what level of access each person would actually require.

The growing use of cloud applications can also raise security risks around identity. Organizations are turning to cloud applications because they are often cheaper than internal applications and can be adapted more easily. Colleges and universities are no exception and are increasingly relying on the cloud to not only manage the school's operations but also deliver education through online classes, for example. But organizations do not own these third-party applications and are thus limited in their ability to apply their security protocols, such as who has access to the application and what privileges employees can have once they gain access.

[4] GBI investigating cyber-attack at *Augusta University.* September 13, 2016. WRDW12 Web site. http://www.wrdw.com/content/news/Augusta-University-employees-fall-prey-to-cyber-attack-393190941.html

Why IAM is a challenge for higher education

When it comes to implementing IAM policies and programs, colleges and universities face a number of obstacles.

First, schools must manage a huge number of identities for students. According to the National Center for Educational Statistics, some 20.5 million students were expected to attend American colleges and universities in the fall of 2016.5 Harvard enrolls about 22,000 undergraduate and graduate students. Penn State University enrolls around 40,000 undergraduates.6 And the University of Central Florida enrolls around 55,000. These numbers rival the population of small cities.

And this student population undergoes a major revision twice a year. Each fall, incoming freshmen must be given access to a school's network. In the spring, an almost equal number of seniors graduate. And while graduates may no longer be active students, colleges and universities diligently work to keep alumni engaged, for fund-raising, for example. Therefore, schools may want their graduates to retain some level of access as well.

In addition to these large student populations, colleges and universities must also manage the identities of their faculty and administrative staff. Moreover, schools may also want to give access to certain individuals outside their immediate community, such as guest lecturers or prospective students.

These large numbers of identities are only part of the story, however. In an enterprise, employees typically have one role in their organization and therefore need only one identity and one level of access. But in a college or university, many in the community have multiple roles or "personas," which can greatly complicate the task of assigning user-identity standards. For example, a graduate assistant may be considered both a student and a faculty member. A professor may teach at one school and be a guest lecturer at another. He can also be an alumnus. A doctor that teaches at a university hospital could also become a patient. Each of these roles or personas would generally have different levels of access.

The age and level of sophistication of a school's technology can also present challenges. Universities and colleges can have multiple networks and systems that are siloed and difficult to integrate. For example, the law school may have its own system, which is separate from the graduate school, which itself is separate from the undergraduate college. Sometimes these systems were developed in-house years ago and are now outdated, making them difficult to modify and upgrade.

Finally, enforcing common-sense security practices can be a challenge in a university setting. Students sharing passwords or leaving passwords and usernames where they can be readily seen can make access to networks easy work for bad actors.

[5] National Center for Education Statistics. "Back to school statistics." Web site http://nces.ed.gov/fastfacts/display.asp?id=372

[6] 10 Universities With the Most Undergraduate Students. U.S. *News & World Report*. September. 22, 2016. http://www.usnews.com/education/best-colleges/the-short-list-college/articles/2016-09-22/10-universities-with-the-most-undergraduate-students

Questions for college IT administrators about IAM

- Do you know who has access to what data/function?
- Is this access appropriate (how did they get it)?
- Can someone access more than they need?
- Do you have accountability for the operating system and infrastructure access?
- Where does your sensitive data reside and who owns it?
- Are there combinations of access that could be “toxic”?
- How are people using your data and can you prove it?
- Do you have access- related compliance liabilities?

KPMG

What colleges and universities need to do

Given the spike in cyber attacks, college and university administrators are becoming increasingly concerned about the vulnerability of their IT systems. According to KPMG's 2015-16 Higher Education Industry Outlook Survey,[7] 47% of respondents said that cyber risk was the emerging trend affecting their institution the most.

Improving their identity access management can help schools enhance their cyber risk prevention programs. Here are some steps school administrators and IT departments can begin to take to address IAM issues:

- Determine a single authoritative source to become the system of record for all user information related to identity for the school's population. This source could be the system aligned with human resources or a student database, for example.
- Determine the common standards that constitute a user identity, that is, the characteristics that identify a user as an individual person (for example, first name, last name, user ID, password, school enrollment, class registrations, year of graduation, etc.).
- Create a database of records for all the faculty, staff, students, alumni, and other persons (guest professors, etc.). This database now becomes the go-to authoritative source for any questions about who a person is.
- Determine the most-sensitive information systems that the user populations have access to, such as information that falls under regulatory mandates (e.g., HIPAA and PII), and systems that process financial and other personal information or systems that house data being used for proprietary research.
- Determine the level of access for each person in the authoritative source to the information in those systems to gain control around user access. Identify the high-risk users, users who may have elevated access, users who may have privileged accounts on a restricted network that need to be monitored, and users who may need to have their access curtailed if they have mistakenly gained permissions beyond their role. The idea is that users should be given the least privilege necessary.
- Implement a governance system and automate processes whenever possible. For example, students can be given a PIN to set up their account after verifying their identity with a driver's license or other means.

[7] KPMG 2015-16 Higher Education Industry Outlook Survey
http://www.kpmg-institutes.com/institutes/government-institute/articles/2015/11/2015-2016-higher-education-industry-outlook-survey.html

Other benefits

In addition helping to guard against cyber attacks, IAM offers colleges and universities several other benefits:

- IAM helps institutions identify high-risk users, that is, users who have a certain level of privileged access that may enable them to cause damage to the institution.
- IAM enables schools to identify segregation of duties (SOD) violations—the classic example being the user who has access to accounts payable and accounts receivable. IAM can enable administrators to remediate these SOD violations quickly before they can do damage.
- IAM will clean up rogue access, as there will be a number of accounts that are no longer needed. For example, accounts that remain active even though the students graduated years ago. In addition to enhancing cybersecurity, cleaning up these accounts can result in cost savings if the school is licensing software based on the number of its accounts.
- IAM can also help institutions to achieve operational efficiencies and cost reductions by automating legacy manual business processes, where accounts have to be manually provisioned. Such automation can also reduce the risk of inappropriate access being granted as a result of human error.

31
32
33
51

Final thoughts

Colleges and universities, with their rich and often decentralized storehouse of personal and financial information about students, research and other data, are prime targets for cyber criminals. And school administrators can expect attacks to intensify as hackers become even more resourceful.

IAM gives colleges and universities a consolidated way to establish the rules, procedures, and underlying technology to efficiently manage user access, ensuring the right people have the right access to the right information at the right time.

Authors and contributors

Charles Collier

Charles Collier is a principal in KPMG's Public Sector Advisory practice, specializing in organizational transformation services. He has more than 25 years of experience with transformation, system modernization, change management, shared services, outsourcing transactions, in-sourcing, business requirements definition, analysis of alternatives, program management, governance, quality assurance, and independent verification and validation. Charles has successfully managed major system implementations and organizational transformation programs at more than 75 organizations. In addition, Charles has worked with numerous institutions of higher education including the University of Texas, Pennsylvania State System of Higher Education (PASSHE), and California State University System (CSU) on IT Modernization, Shared Services, Transformation, and Cyber Security projects.

Prasad Jayaraman

Prasad Jayaraman is a principal in KPMG's Advisory practice with more than 17 years of experience in identity management practices, as well as substantial experience in technology professional services, technology consulting, and medical technologies. Prasad has served as a chief executive officer with responsibility for overall leadership, growth, direction, and culture in the information and technology services sector. He has also served as a vice president for business development and global head of identity management practices, responsible for all aspects of integration, including sales, alliances operations, human resources, and service delivery.

Scott Jolly

Scott Jolly is a solution relationship director in KPMG's IT Advisory practice with more than 15 years of identity management and security advisory experience. He has a strong background in hands-on delivery, project delivery, and solution selling. Scott's current and past clients include the U.S. Department of Defense, as well as a large cross section of the financial services, higher education, and healthcare sectors. Scott has worked on a number of IAM projects at wide range of schools, including two Ivy League institutions, two large State Universities, as well as several smaller colleges in the U.S.

Toby Emden

Toby Emden is a managing director within KPMG's Cyber Advisory practice, specializing in IAM strategy, architecture, and implementation. He has 17 years' experience leading high-performing information security teams, developing IAM governance frameworks, and implementing complex identity solutions across a wide range of industries, including financial services, healthcare, information technology, higher education, media/entertainment, and energy. As the former chief security architect and IT security portfolio lead for a FORTUNE 50 financial services company, Toby is intimately familiar with the organizational, technical, and business challenges associated with delivering security transformation programs within the modern enterprise. Toby has led IAM programs and provided executive advisory services for several of the largest universities in the U.S.

Ken Dunbar

Ken Dunbar is a director in KPMG's Advisory practice with more than 20 years' experience in information protection, including IAM strategy. He has led multiple large-scale projects to uplift legacy IAM systems. He has also delivered IAM strategy road maps, taking into account new disruptive trends such as mobility, hybrid cloud infrastructures, privileged account management, and shadow IT applications. He is a thought leader in cybersecurity frameworks accounting for organizational changes and governance-centric deployments. In addition, Ken has managed IAM implementation projects at several large state and private universities.

About KPMG

KPMG has been a leader in providing services to higher education for over 80 years. In fact, KPMG was the first major professional services firm to develop a higher education practice to specifically serve these institutions. Our professionals not only have the commitment and dedication, but also the firsthand knowledge of, and in-depth experience with, the issues and challenges that face higher education institutions.

The challenges facing higher education institutions have grown rapidly. Whether in industry journals, conferences, board meetings, or staff meetings, leaders increasingly express concerns that existing approaches to the delivery of program services by higher education and institutions no longer provide a reliable path into the future, and that they must consider new approaches. KPMG aims to help define the unique path to success by addressing common concerns—among them, those associated with cybersecurity.

Identifying and protecting critical assets in the face of a constantly evolving threat landscape is essential. KPMG's Cyber practice is dedicated to helping clients identify their most important information assets, and works with them to develop an effective and efficient approach that focuses on people, process, and governance as a foundation for technology enablement. KPMG works with several colleges and universities, developing a range of leading digital identity services to help reduce the risk of identity-related breaches.

Contact us

Charles Collier
Principal
T: 512-320-5280
E: ccollier@kpmg.com

Prasad Jayaraman
Principal
T: 408-367-5685
E: prasadjayaraman@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.