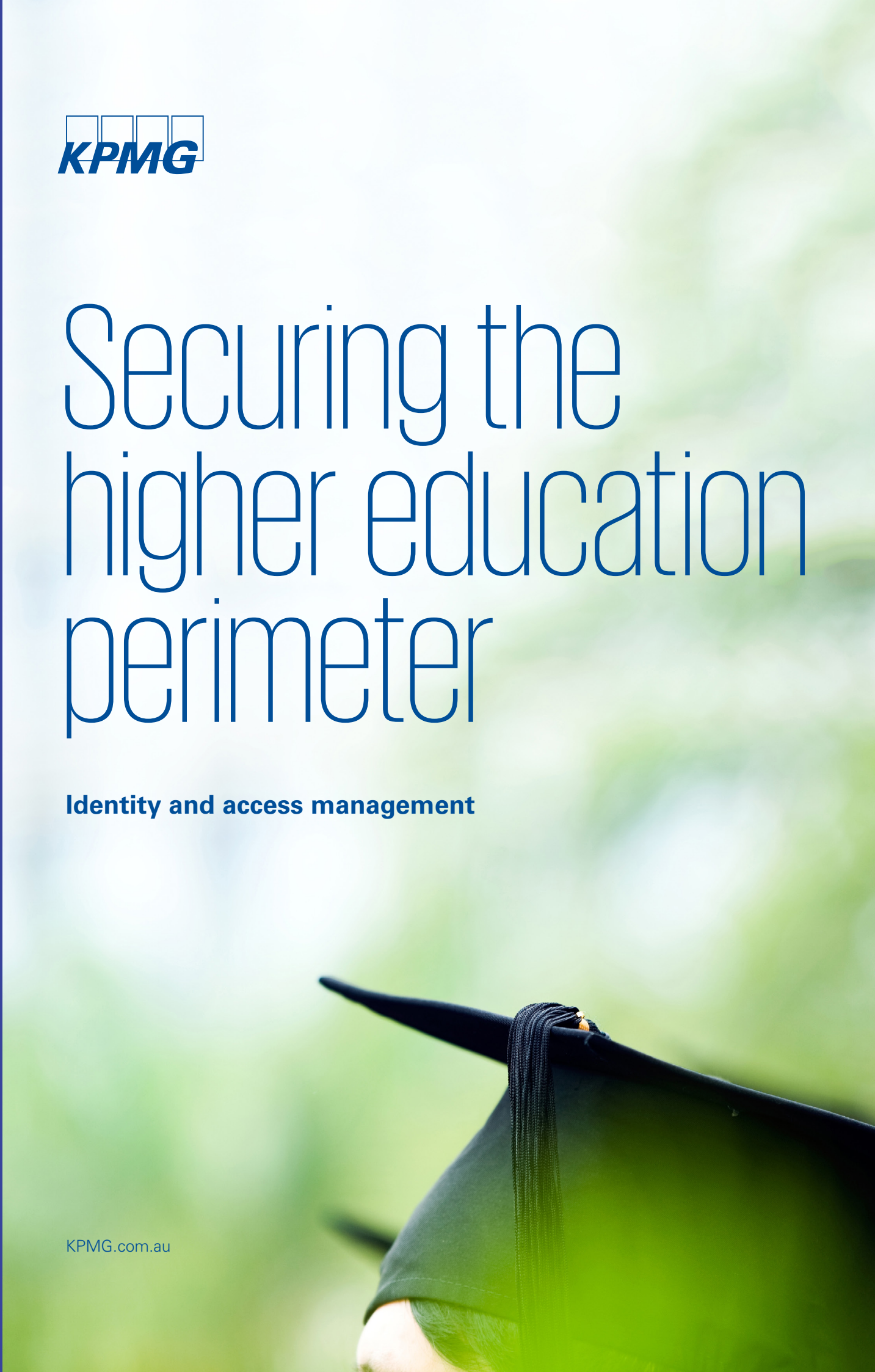
KPMG

Securing the higher education perimeter

Identity and access management



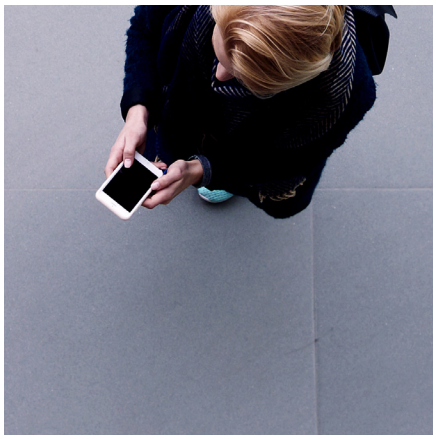
KPMG.com.au

"Hostile cyber activity is a real threat to Australia and its higher education sector. Controlling who has access to universities' networks, systems and applications is an important step in the defence of their information assets and intellectual property."

Jan Zeilinga,
Director, Cyber Security Services, KPMG Australia

Introduction

Each year, tens of thousands of young people begin their studies at universities and higher education providers around the country. Until recently, these incoming students would receive a student handbook to get them started on their university journey. Today, they get an e-mail asking them to create their username and password to gain access to the institution's network. With that, they can register for subjects, sign up to tutorials, network with fellow students and manage their fees.



Like most organisations, universities rely on their internal computer networks to operate effectively. But when it comes to managing access to their systems, higher education institutions face a number of unique challenges. In addition to the influx of new students, a similar number of graduates embark on postgraduate study or the world of work. University staff often have multiple roles requiring separate access levels. Visiting academics need access to the university's network for a time, but need to 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 cyber security challenge, with the risk of identity theft by hackers who want to gain access to a university's networks.

Universities present rich targets for cyber criminals, so that risk is very real. Students provide their institutions with significant amounts of personal and financial information. In addition, larger organisations, often in partnership with private enterprises, engage in proprietary academic 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 education. A number of high profile universities overseas have fallen victim to threat actors. Attacks on universities 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 cases, the typical way in has been through a stolen identity. To protect themselves, universities must proactively uncover where the greatest identity risks reside and consequently which individuals and accounts need to be watched.

To do so, universities need to have a thorough understanding of user identity and levels of access, so they can begin to uncover malicious or anomalous behaviour before it becomes a problem.

One way universities can better protect themselves from cyber attacks is to implement a comprehensive program for Identity and Access Management (IAM) that can be applied to all staff, faculties, 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, universities can help limit cyber attacks by building a more secure perimeter around their networks.

Why hackers like to go to university

Hackers are increasingly focusing on universities as targets for their cyber attacks. In 2013, one leading Australian university was the target of a 'concerted effort' to hack its systems, forcing the shutdown of 25 of its servers. In June 2017, the University College London was hit by a ransomware attack which brought down its shared drives and student management system. The attack is believed to have been launched via a phishing email.

Gordon Archibald, Partner, Cyber Security Services, KPMG Australia, advises that in today's business world "data is the currency in security" and data is the prime focus of many threat actors. This makes universities an enticing target for cyber criminals. Consider that in one breach, hackers can have access to thousands of student IDs, Tax File numbers, bank accounts, credit cards, and Medicare information. 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. Many universities work on large research projects for government or the private sector, and have critical IP which is another rich target. Threat actors wanting to gain access to these projects might include business competitors and criminals seeking intellectual property, or even state actors looking for national security information.

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

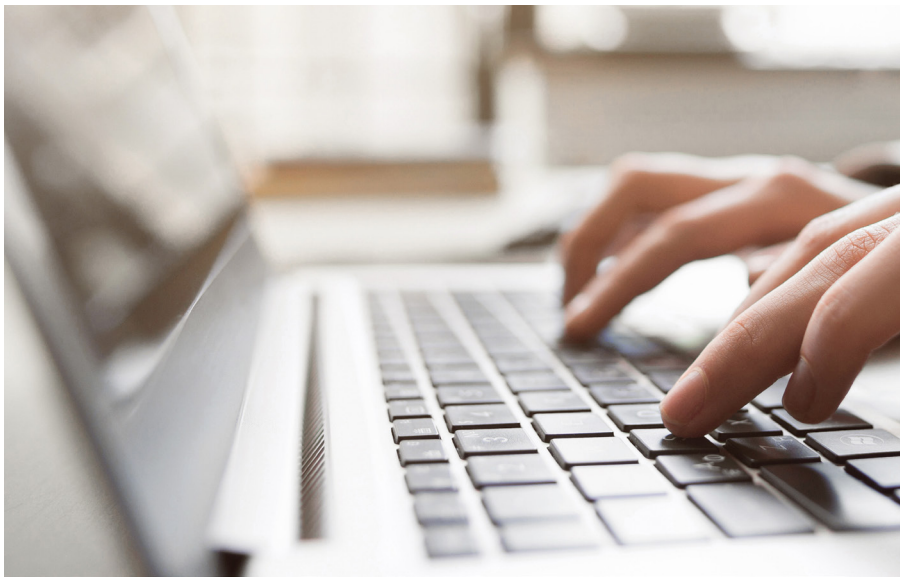
Professor Stephen Parker, a former university vice-chancellor and now National Education Sector Leader at KPMG Australia, warns of the potential risk to the sector:

"Higher education is hugely significant to the Australian economy; universities account for about $30 billion in revenue. International education from all sectors, but mainly higher education, contributes about $22 billion to the economy, and is our third largest export market. New mandatory data breach laws which have made reporting cyber attacks or technical failings compulsory, pose a significant reputational risk for universities. Prospective international students can and will find out about IT breaches at Australian education providers."

Breaches can be costly as well. According to the Ponemon Institute, the average global cost of data breach per lost or stolen record in education was US $246.

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 university was able to retrieve the data from backup systems, but they did pay the ransom of US$15,000 as a precaution. In addition to the upfront costs, leaked research can expose proprietary information, leading to long term financial loss and the potential withdrawal of grants and contracts.

How hackers get in



"In today's business world data is the currency in security, and data is the prime focus of many threat actors. This makes universities an enticing target for cyber criminals."

Gordon Archibald,
Partner, Cyber Security Services,
KPMG Australia

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, a large Australian university fell victim to a phishing scam resulting in a user account in the Credit Management area being compromised, and sending messages to former students. Although the impact of this breach was minor and quickly contained, the compromised user account was active for a couple of days, showing how easily accounts can be infiltrated.

In other cases, identities can be stolen because of lax policy or the failure of individuals to follow cyber security measures.

According to the Council of Australian University Directors of Information Technology (CAUDIT), universities face cyber security threats from ever increasing sources. With the vast range of access points across a campus and large number of critical data assets, personal information, valuable research and intellectual property are potentially vulnerable.

Because they are easy to use and readily available, these external storage services can be a great temptation for faculty and students if the university's network is not easily accessible.

Another attack vector is sometimes called the 'phone-a-friend' scenario. For example, a new staff member joins a university's research team. Her 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 employee 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, and then move on at the end of the semester.

Yet another way 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 students 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. Organisations are turning to cloud applications because they are often cheaper than internal applications and can be adapted more easily. Universities are no exception and are increasingly relying on the cloud to not only manage operations but also deliver education through online classes, for example. But organisations need to ensure they integrate these cloud applications into a secure IAM solution to protect the data as they move to hybrid or fully cloud architectures.

Why IAM is a challenge for higher education

When it comes to implementing IAM policies and programs, higher education institutions face a number of obstacles. First, universities must manage a huge number of identities for students. According to the Department of Education, a total of 1.4 million students attended Australian universities in 2015. Monash University enrols about 56,500 undergraduate and graduate students. The University of Sydney enrols around 48,000. And Curtin University in Western Australia enrols around 47,000. These numbers rival the population of small cities.

And this student population undergoes a major revision twice a year. At the beginning of each year, incoming students must be given access to a university's network. Yearly, an almost equal number of students graduate. And while graduates may no longer be active students, universities diligently work to keep alumni engaged, for future study opportunities, for example. Therefore, institutions may want their graduates to retain some level of access as well.

In addition to these large student populations, universities must also manage the identities of their academic and administrative staff. Moreover, institutions 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 organisation and therefore need only one identity and one level of access. But in a university, many in the community have multiple roles or 'personas', which can greatly complicate the task of assigning user-identity standards. For example, a research assistant may be considered both a student and a faculty member. A professor may teach at one faculty and be a guest lecturer at another. They could 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 university's technology can also present challenges. Universities 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 engineering school, which itself is separate from the undergraduate part of that same faculty. Sometimes these systems were developed in-house years ago and are now outdated, making them difficult to modify and upgrade.

"New mandatory data breach laws which have made reporting cyber attacks or technical failings compulsory, pose a significant reputational risk for universities. Prospective international students can and will find out about IT breaches at Australian education providers."

Professor Stephen Parker AO
National Sector Leader, Education,
KPMG Australia

"The focus for universities and higher education providers should be around agility in technology and a move to cloud-based solutions and platforms. A good identity management solution will enable this transition, reducing integration issues, while at the same time increasing security."

Dr Julian Edwards,
Partner, Technology Enablement, KPMG Australia

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.

Questions for university 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?

What the higher education sector needs to do

Given the spike in cyber attacks, university administrators are becoming increasingly concerned about the exposure of their IT systems. According to KPMG America's 2015-2016 Higher Education Industry Outlook Survey, 47 percent of respondents said that cyber risk was the emerging trend affecting their institution the most.

Improving their identity access management can help universities enhance their cyber risk prevention programs. Here are some steps 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 university'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, university enrolment, subject enrolments, year of graduation etc.).

Create a database of records for all the faculty, staff, students, alumni, and other persons (guest academics 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 mastakenly 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 Medicare or OSHC card or other means.

Other benefits

In addition helping to guard against cyber attacks, IAM offers 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 institutions 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 cyber security, 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.

In summary

Higher education institutions, with their rich and often decentralised storehouse of personal and financial information about students, research and other data, are prime targets for cyber criminals. And education administrators can expect attacks to intensify as hackers become even more resourceful. IAM gives 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.

Contact us

Gordon Archibald
Partner,
Cyber Security Services
KPMG Australia
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

Professor Stephen Parker AO
National Sector Leader,
Education
KPMG Australia
T: +61 3 9288 5901
E: parkers@kpmg.com.au

Dr Julian Edwards
Partner,
Technology Enablement
KPMG Australia
T: +61 2 9335 8844
E: jmedwards1@kpmg.com.au

Jan Zeilinga
Director,
Cyber Security Services
KPMG Australia
T: +61 2 9335 7162
E: jzeilinga@kpmg.com.au

KPMG.com.au