Whitepaper

Technology report

Access control in higher education

Contents

HID Global commissioned SecurityInformed.com to produce this document, which is based on research conducted jointly by HID Global and Genetec.

About the author
An experienced journalist and long-time presence in the U.S. technology marketplace, Larry Anderson is the Editor of digital publications SecurityInformed.com and SourceSecurity.com. Mr. Anderson is the websites' eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to the two sites. From 1996 to 2008, Mr. Anderson was editor of Access Control & Security Systems magazine and its affiliated websites. He has written numerous articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in journalism from Georgia State University with a minor in marketing.

1

Survey Results

Access control is a fundamental element of security in higher education, impacting every department and every stakeholder throughout an institution. However, costs are an obstacle, and many aging access control systems urgently need to be upgraded. Managing systems can also be a challenge, although there are new technology options that can make life easier for administrators as well as those who use the systems.

HID Global and Genetec commissioned a survey to provide insights about access control in the higher education market. This report will highlight the results of that survey with additional commentary.

> “Safety and security are an important aspect of a student’s university experience. An unsafe environment will encourage students to seek alternatives.”

What Is At Stake

In general, colleges and universities are seeking to embrace more technology as a way of improving their operations and even to attract students. This desire helps to drive discussions of access control in higher education. As always, security is a major concern among parents and prospective students as they choose where to study.

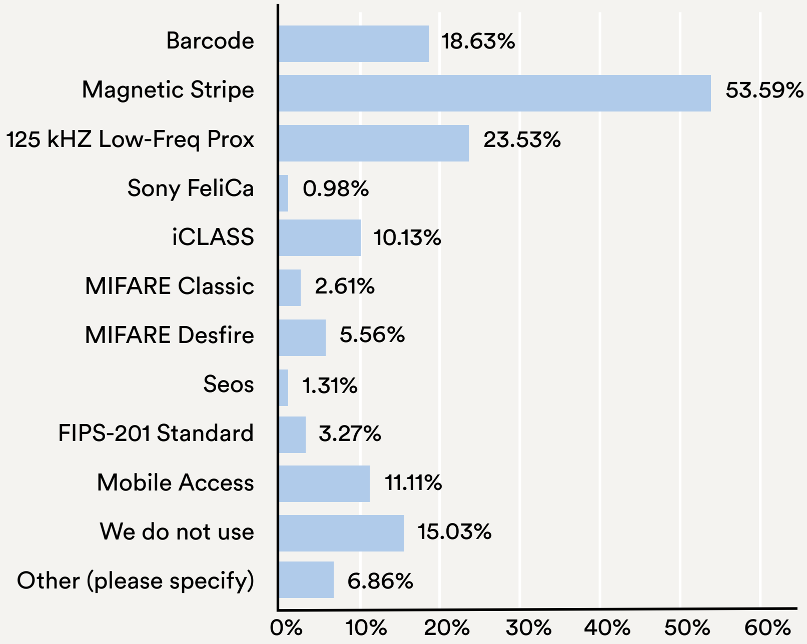
“There are students making choices about where they are going to school based on the access control technologies that are used,” says JasonFriedberg, Genetec’s North America Business Manager for Education. “For example, a mobile credential suggests a more tech-savvy campus.”

One survey respondent put it succinctly: “Safety and security are an important aspect of a student’s university experience. An unsafe environment will encourage students to seek alternatives.” Another respondent adds: “More security [is] more retention and enrollment.”

About Current Systems

Older technologies such as barcode, Magnetic Stripe (mag stripe) and 125khz low-frequency Proximity (Prox) continue to dominate physical access control systems in higher education. More than half of survey respondents still use mag stripe, and almost a quarter still use 125khz Prox.

Which credential technologies does your organization support for physical access control? (check all that apply)



Although still popular in higher education, mag stripe and low-frequency Prox are less secure than newer options such as smart cards or even mobile access, says Brett St. Pierre, HID Global's Director of Education Solutions. "Updating readers in new buildings or retrofitting to existing buildings is a cost-effective way of implementing newer technologies even if funds are not available to replace a total system," he adds.

Systems are also aging. For example, the survey shows 33.76% of readers are more than six years old; 30.6% of controllers and 24.0%

> "Updating readers in new buildings or retrofitting to existing buildings is a cost-effective way of implementing newer technologies even if funds are not available to replace a total system."

How old are the following components of your current access control system?

	<1 year	1-2 years	2-4 years	4-6 years	6+ years
Readers	7.26%	14.96%	21.37%	22.65%	33.76%
Credentials	14.72%	21.65%	25.97%	16.02%	21.65%
Controllers	7.76%	14.22%	26.29%	21.12%	30.60%
Software	13.73%	20.17%	25.75%	16.31%	24.03%

When do you plan to upgrade components of your current security system?

	<1 year	1-2 years	2-4 years	4-6 years	6+ years
Access Control (readers, credentials, controllers, etc.)	9.44%	33.91%	25.75%	12.02%	18.88%
Video Surveillance (cameras, software, etc.)	16.81%	29.74%	22.84%	12.50%	18.10%
Alarms/Notification Systems	13.97%	27.07%	22.27%	14.41%	22.27%
Visitor Management	16.96%	29.13%	20.43%	13.04%	20.43%
Network Security	28.95%	27.19%	21.49%	6.58%	15.79%

of software are also more than six years old. The largest percentage of upgrades are planned in the next 1-to-2 years; network security upgrades are planned sooner, at 28.5% in less than a year.

“College campuses will use a system until it dies,” comments Friedberg. “They keep it running as long as possible. It’s like plumbing – you unstop the drain, you don’t replace all the pipes.” Campuses might keep an inventory of system components on a shelf to switch out as needed for older systems.

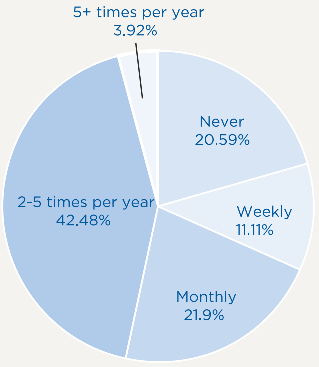
Another issue is the number of disparate systems – of various ages – in operation at a typical higher education institution, says Friedberg.

With residence halls, multiple buildings and athletic facilities, an institution may have a half dozen or more systems. None of them are integrated. Operators might have to log into several different systems to respond to a single incident.

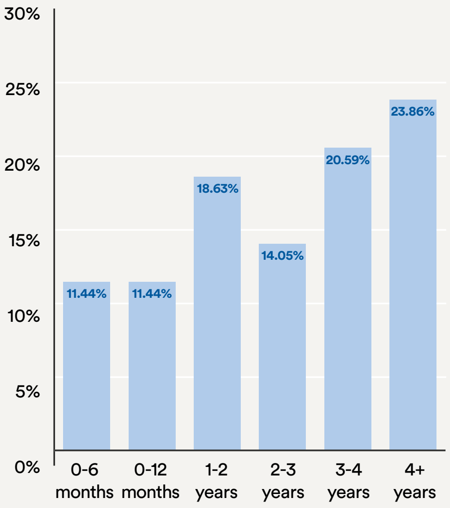
Older systems are less dependable. Some 42% of survey respondents say their current access control system malfunctions two to five times per year; another 22% estimate their system malfunctions monthly.

On average, 22.9% of respondents say access control cards at their campus are used for 12 months or less (total of responses for 0-6 months and 6-12 months); another 23.9% say cards are used four years or more. The rest fall somewhere between the extremes.

How often do you experience malfunction incidents with your current access control system?



Approximately how long is the average access control card used at your campus?



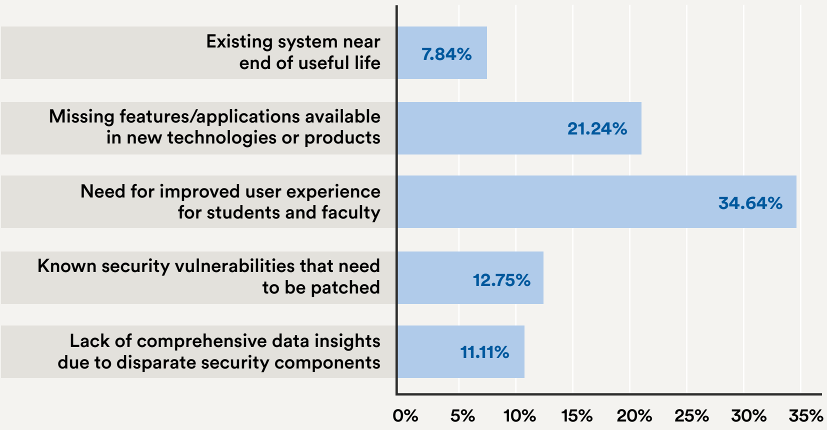
2

Challenges for Higher Education

The top access control challenge faced by higher education is to improve the user experience for students and faculty, according to the survey. The next biggest challenge is missing features that are available in newer technologies.

> “Managing credentialing and privileges, especially among the student population, is a difficult and recurring task for system administrators.”

What is the biggest challenge you face with your current access control system?



The most inconvenient aspects of current systems to system administrators are:

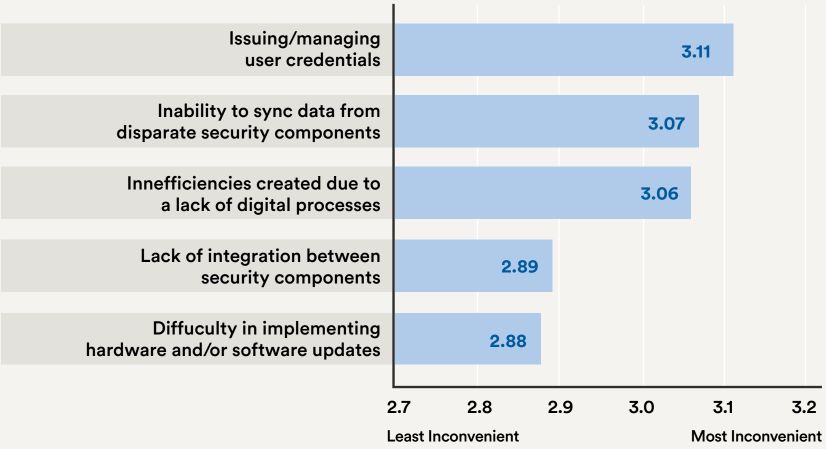
1) issuing/managing user credentials

2) inability to sync data from disparate security components

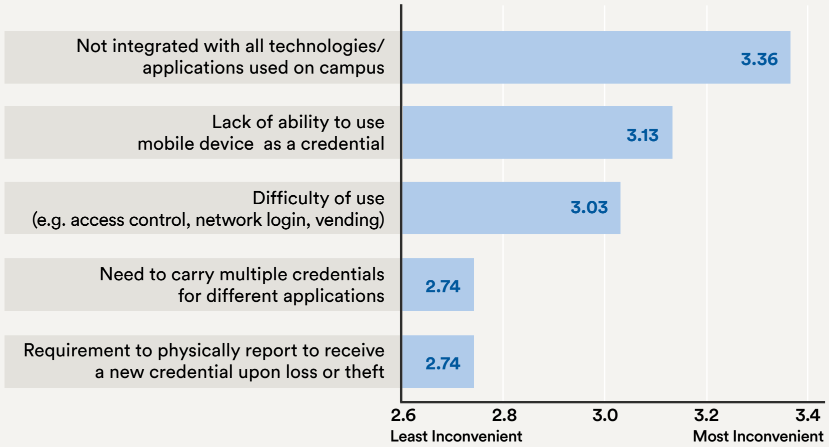
3) inefficiencies created due to a lack of digital processes

Managing credentialing and privileges, especially among the student population, is a difficult and recurring task for system administrators, says Friedberg. In a typical college access control system, there may be hundreds of groupings with various privileges. Furthermore, it all starts over every semester, with little institutional memory over time.

What are the most incovenient aspects of your current access control system to you as a security administrator?



What are the most incovenient aspects of your current access control system to students and faculty?



> “Around 30% of respondents report more than 10% or more of cards are lost on their campuses each year.”

The most inconvenient aspects of current systems to students and faculty are:

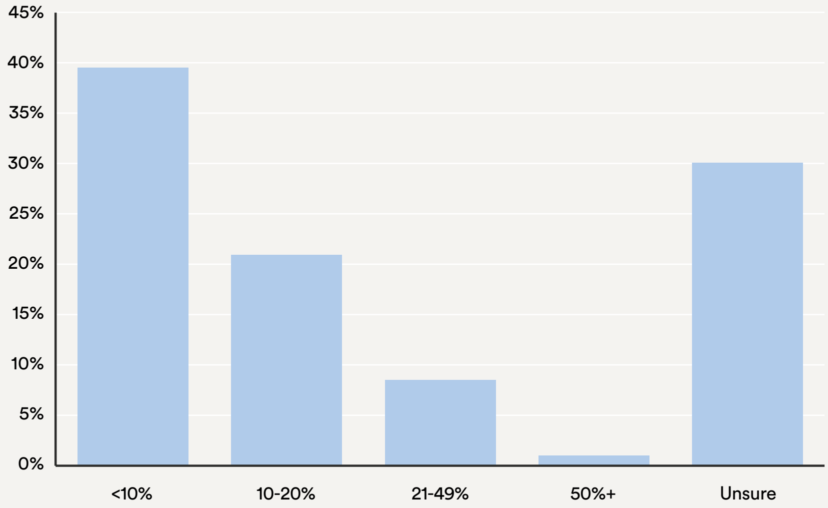
1) not being integrated with all technologies/applications used on campus

2) lack of ability to use mobile device as a credential

3) difficulty of use: e.g., access control, network login, vending

Lost credentials are also a problem. Around 30% of respondents report more than 10% or more of cards are lost on their campuses each year.

Approximately what percentage of access control cards is reported lost on your campus each year?



Drivers And Obstacles

Top drivers for upgrading access control systems listed by survey respondents (in order) are:

1) to improve user convenience

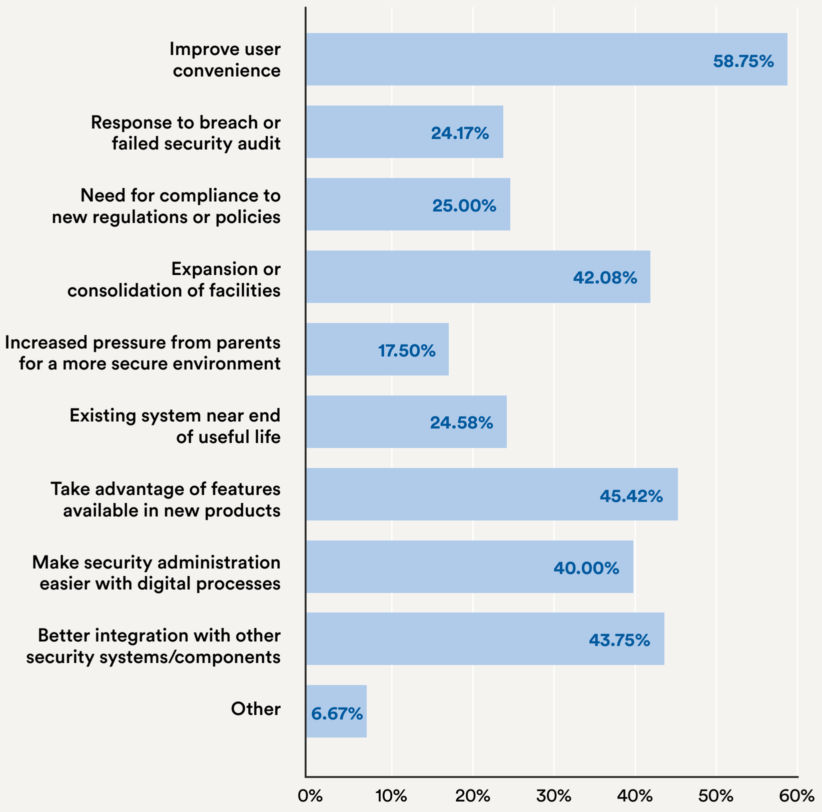
2) to take advantage of new technology features

3) better integration

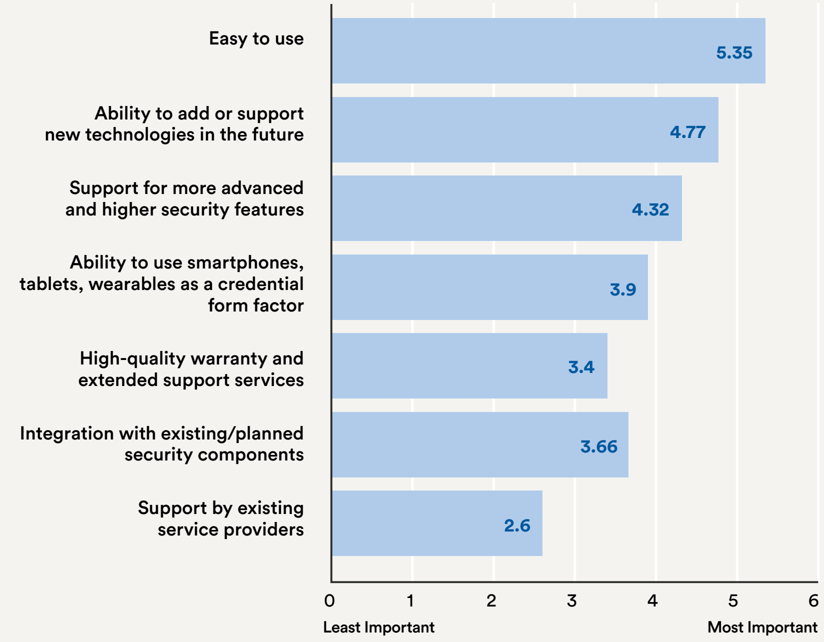
4) expansion or consolidation of facilities

Especially in the higher education environment, user experience often equates to more security, says St. Pierre. College students, even more than other user populations, are likely to seek out ways to bypass systems that are inconvenient to use. Propping doors open or leaving windows unlocked negate the intent of access control systems, but are a reality for impatient college students who can't be bothered with systems that are difficult to use. "College students will find the easiest way around a system," says Friedberg.

Which factors have been drivers to upgrade your current access control systems? (choose all that apply)



Rank the following benefits you seek when installing a new access control system.



Top expected benefits from installing a new system include:

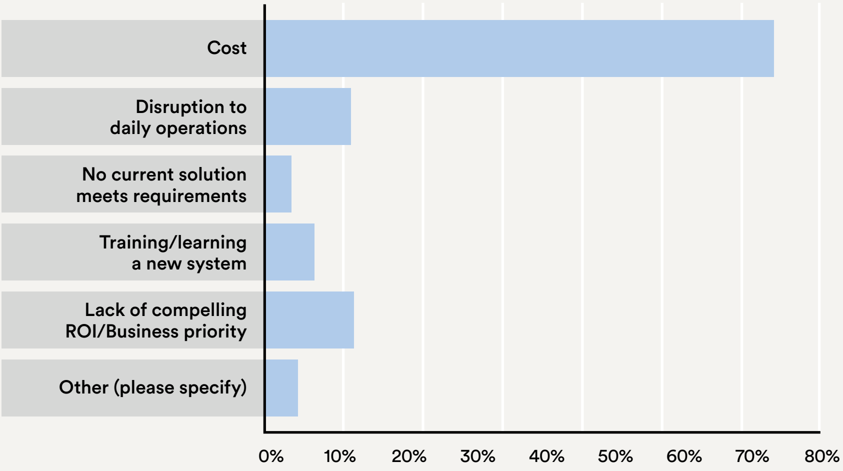
1) easy to use

2) ability to add or support new technologies in the future

3) support for more advanced and higher security features

4) ability to use smartphones, tablets and wearables as a credential form factor

What is the biggest obstacle to upgrading your access control system?



> "After systems are installed, ongoing costs may be lower than those of legacy systems because additional capabilities of newer systems increase operational efficiencies."

By far the biggest obstacle to upgrading is cost (64%). Lesser obstacles are lack of a compelling ROI/business priority and disruption to daily operations. Unfortunately, many institutions migrate to systems that fulfill minimum requirements because of cost, says Friedberg.

Cost is seen as an obstacle, but value is often not factored in. "The bigger issue is value, not cost," says St. Pierre. "It's not that they don't have the money, but they are spending it in areas where there is more return on the investment. In universities, we're seeing fast-moving and evolving threats and user experience enhancements. These factors increase the value of systems without increasing the costs. Costs are fixed, but the evolving market provides more benefits." After systems are installed, ongoing costs may be lower than those of legacy systems because additional capabilities of newer systems increase operational efficiencies, he adds.

3

New Opportunities

Almost half of respondents either use two-factor authentication on their campus or plan to implement it in the future. Slightly more than half (51.3%) have no plans to implement two-factor authentication.

Two-factor authentication is most often implemented for more highly secured areas of a university, such as a research facility or biochemical laboratory. Two factors may also be employed when there is a likelihood of shared credentials, or if there is a specific security concern, such as a residence hall located near the campus perimeter that is at risk from trespassers, according to St. Pierre.

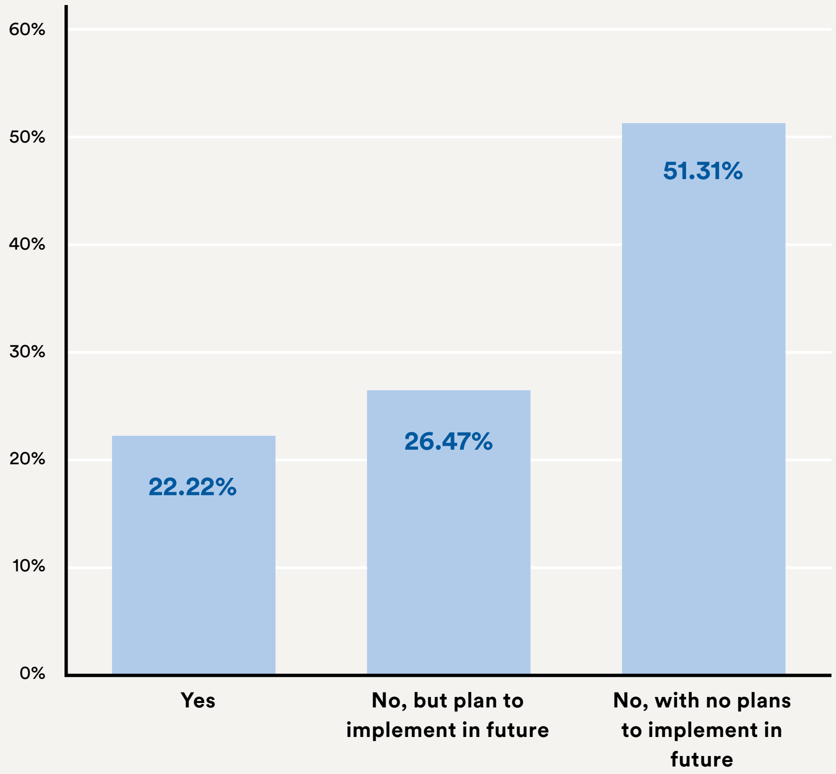
A challenge is the variety of companies that produce systems for the various applications, and the need to standardize those systems to interface with a single credential.

Some 54.2% of respondents would be interested in using their access control credentials to support multiple applications beyond physical access. Another 30.8% are unsure.

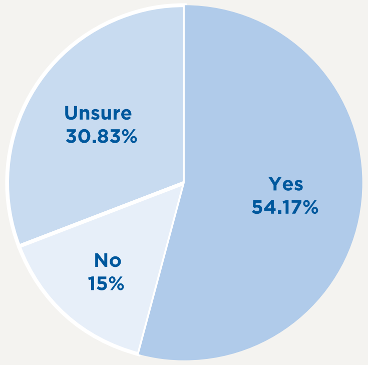
There are currently more multi-use applications in the higher education market than any other, says St. Pierre. Most colleges and universities want their students to use cards as much as possible, and many institutions are developing innovative applications such as locking bicycles and providing lockers for skateboards. Card technologies exist to support other uses from checking out books to paying for food as well as accessing dormitory rooms and many more, he says. A challenge is the variety of companies that produce systems for the various applications, and the need to standardize those systems to interface with a single credential.

"It requires buy-in from multiple departments. Not just the card office for security, but buy-in from food services, vending, the laundry company, etc.," says Friedberg.

Are you currently using two-factor authentication (e.g. smart card + PIN) on your campus?



Would you be interested in your access control credentials supporting multiple applications?



> “Existing infrastructure will have to upgrade fast, but it is rare that we see an institution install a system today without thinking ahead toward the inevitability of mobile access control”

Achieving The Reality Of Mobile Access Control

Mobile access control is ranked as an important new application. Other desirable applications in higher education include secure printing, network access and point-of-sale/cashless vending. [See graph on the next page.]

Mobile access control is more appealing in the higher education market than any other, given students’ affinity for their smartphones, Apple watches, and/or wearable technologies. Students grew up in an age when the smartphone has been the center of their lives, so they would expect to use a smartphone as an access control credential. There are also advantages to system administrators, who can deliver credentials remotely and save expenses of replacing cards. And there is better security: Students are less likely to loan their smartphone than their access control card.

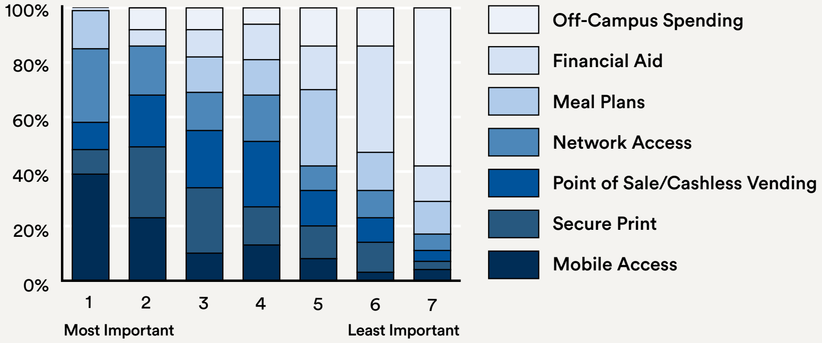
St. Pierre says infrastructures are transitioning to support mobile access technology, and mobile will be the credential of choice in the next five to seven years. “Existing infrastructure will have to upgrade fast, but it is rare that we see an institution install a system today without thinking ahead toward the inevitability of mobile access control,” he says.

Specifically, a high percentage of universities are investing in readers and locks with Bluetooth technology, says Brandon Arcement, HID Global’s Director of Product Marketing. Also, access control apps are a logical extension of the college and university trend toward developing apps for everything from registration to communicating with professors.

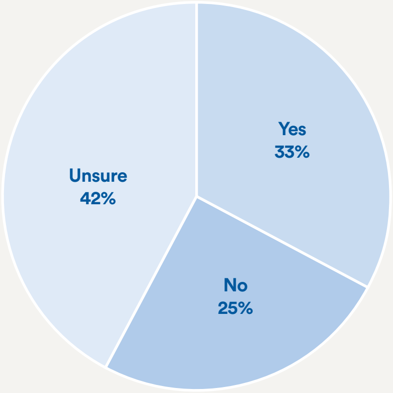
Some 33% of respondents say they would be interested in implementing Real Time Location Systems (RTLS), which is defined as technology that automatically identifies and tracks the location of objects or people in real time. Another 41.9% are unsure. One issue is the frequency of false alarms, says Friedberg. For example, a student walking from a library to a dormitory might be easily distracted, and the delay could trigger a false alarm if he or she did not arrive on time.

Respondents are evenly split – around 36% each – on whether providing credentials to alumni to access facilities will be of growing importance. Another 27.8% are unsure. [See graph on nextpage left] Providing additional access to alumni provides benefits from a fund-raising perspective, and keeps graduates involved in the university community.

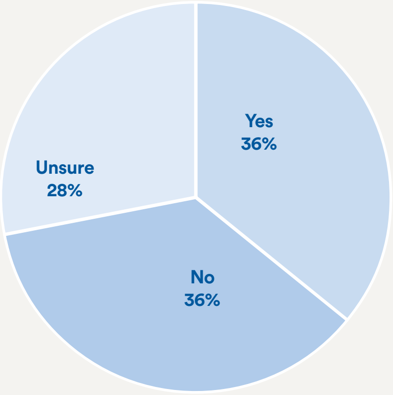
Rank the following applications in order of importance



Would you be interested in implementing RTLS (real time location systems)?

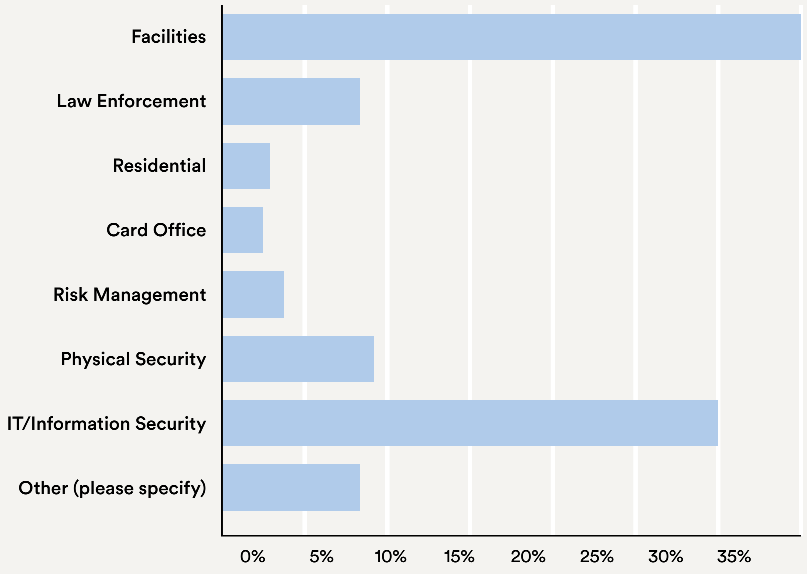


Is providing credentials to alumni of growing importance?



“Campuses survive on alumni giving, and some have billion-dollar alumni funds,” says Friedberg. “If you are a heavy donor, they would love to offer you free admission to a football game or help you feel more connected to campus. But how can it be managed?”

Which department is primarily responsible for budget decisions related to access control system upgrades?



The Buying Decision

Facilities departments or information security (IT) are most often responsible for budget decisions related to access control system upgrades, although other stakeholders are involved.

Decisions to purchase technology equipment are somewhat seasonal – more likely in the spring and summer and less likely in the autumn and winter. Friedbergnotes that fiscal years end June 30th, so decisions are made in the months right before that, and installations often happen in the summer months.

A Dynamic Market

Taken together, the survey results emphasize the growing and dynamic market for access control among colleges and universities. It’s a market that is full of opportunities to expand the usefulness of systems and to embrace the enhanced capabilities technology has to offer.

"It's a market that is full of opportunities to expand the usefulness of systems and to embrace the enhanced capabilities technology has to offer."

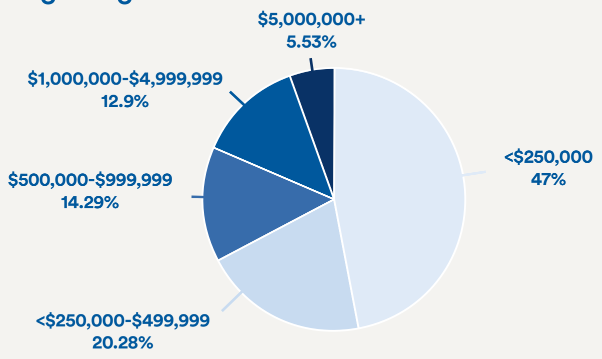
4

About The Survey

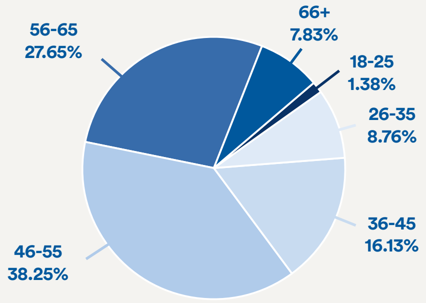
Survey respondents are a diverse group in terms of campus population size (with the largest percentage from campuses of 1,001 to 5,000); serving a variety of security roles within the college or university (with largest share from IT and security); diverse in age (with the largest share from 45 to 65); and overseeing a range of annual budget sizes (although 47% have a budget below $250,000)

In the United States, universities and colleges can compile such statistics using the data that they are mandated to provide to the federal government under the Clery Act.

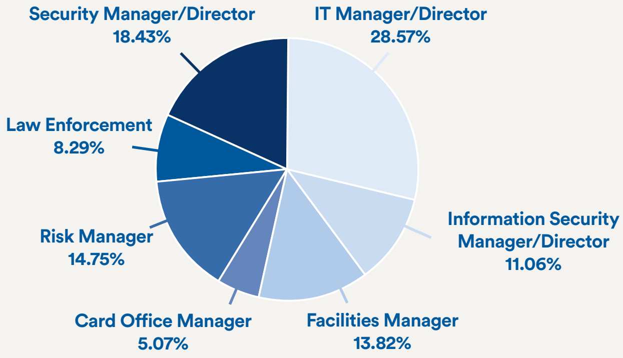
Operating Budget



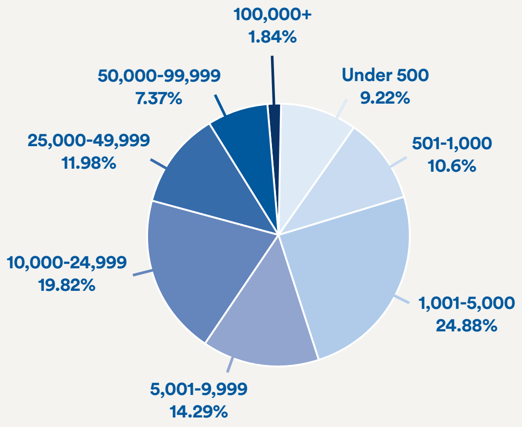
Age



Security Role



Campus Size



About Genetec

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company's flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security, and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montréal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 80 countries.

For more information about Genetec, visit **genetec.com**.

About HID

HID Global is a worldwide leader in trusted identity solutions that power people, places and things. HID solutions give people secure and convenient access to physical and digital places and connect things that can be accurately identified, verified and tracked digitally. Millions around the world use HID products and services to navigate their everyday lives, and over 2 billion things are connected through HID technology. Headquartered in Austin, Texas, HID has over 3,000 employees with offices supporting more than 100 countries. HID Global® is an ASSA ABLOY Group brand.

For more information, visit **www.hidglobal.com**.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

UPDATED: 28-JULY-20