Educational institutions have a responsibility to keep their students safe

STUDENT SECURITY

Dan Meyrick *reports on the challenge of keeping students safe from enrolment to graduation*

From kindergarten to high school and all the way through university, we spend a considerable amount of our lives attending educational institutions. Apart from enabling learning, these vital places have a responsibility to keep their students safe. Unauthorised visitors, theft and increasing acts of violence and terror threats on campuses across the globe have brought school security firmly to the top of the agenda. Yet, the sheer size of many campus areas combined with thousands of students and personnel with varying levels of granted access have proven a real challenge for those attempting to keep educational institutions and their perimeters safe – while offering effective and seamless operations.

Students must be offered the highest degree of security without complicating their daily lives with unnecessary obstacles. But it is not enough to safeguard the classrooms to keep students safe. A comprehensive perimeter security infrastructure needs to be built around them, which not only keeps unwanted people out, but also ensures authorised visitors are granted access to the area in a timely manner, without them feeling unwelcome or unduly stressed by the process.

Educational institutions can have new students enrol, graduate, drop out and attend standalone lectures and events on a daily basis. In order to keep up and grant access on a rolling basis, campus administrators need the right technology to support this process. With the vast size of most campus perimeters, and the number of people needing access to varying areas, it is no longer feasible to expect this all to be done by an admin person behind a counter – at least not if you want this process to run like clockwork. A centralised credential management system streamlines access control operations and manages all cardholder requests from a single location. It can also issue and manage access credentials both to and within the campus area, which brings us to the next – and often overlooked – level of access control.

A campus area houses a wide range of facilities like classrooms, research labs, libraries, sports complexes, teachers' lounges, administrative facilities and sometimes even dormitories. Therefore, having an access control system merely designed to grant visitors entry to the premises is not enough when designing a comprehensive security infrastructure. A person – let's say a student – obviously needs access to the campus, but should by no means be able to access areas designated for teachers or even all classrooms. After a person has been identified and verified as a legitimate visitor, administrators need a system to easily and quickly tick the boxes of which areas they are allowed to access – not only for safety purposes, but for operational efficiency.

UNIFIED SECURITY

Advanced access control is only the outer layer of a rounded security system, however. The next step is to secure the indoor areas, and protect students from a number of potential threats while they're in the building. And this is where a unified security system makes a real difference. Not only does it make access management much easier and quicker, but it also allows those in charge of safety to monitor the entire campus and its facilities without needing to hop from system to system. This increases situational awareness, which in turn allows for faster reaction times to incidents, significantly enhancing overall security. It also cuts security costs, as it helps reduce inefficiencies and administrative costs by allowing operators to monitor multiple sites, even the most remote campuses, from a single location – which has proven particularly valuable to multi-campus educational institutions.

Modern physical security solutions like video surveillance, access control, video analytics and even number plate recognition systems are all aimed at providing campuses the protection they need. However, the way they are managed will be crucial to how effective they'll end up being. When ran separately, these security systems can often cause more headaches than benefits to security officials, as keeping track of them all is highly labour intensive and inefficient. By unifying these security components into a single system, those in charge of securing the campus and its perimeters can rest assured all incidents will be available for them to assess and provide an appropriate response, enabling a more proactive approach to security measures and eliminating time wasted on running systems in siloes.

When an incident occurs, first responders must get the right information to act quickly and effectively. A unified security system can enable information sharing with emergency services when need be, enhancing preparedness by including established connections and communication pathways with relevant law enforcement and other authorities. Having the ability to provide responders with access to video surveillance feeds from the scene of the event can significantly help responders understand all the factors of an emerging incident or event, and thereby help security personnel resolve situations quickly or before they occur. This increased situational awareness can vastly improve campus security and can even save lives in time-sensitive emergency situations.

A modern security solution is designed not only to deliver a unified approach to security operations, but to make everyday life in campus environments run as smoothly as possible. Hosting more than 16,000 students and around 2,500 employees and academic staff, the University of Hull was desperate to upgrade its outdated system into one that could do both. With over 50,000 card holders, access control was at the heart of the upgrade, and it needed one that could be expanded on later with the hardware of its choosing, without being tied to one particular provider. Students, teachers, parents and service people move through education institutions every day – identifying and counting each of them is essential for security, but also for the campus flow. Today's security systems can establish and track access of all campus occupants, lock a facility down in case of an emergency, integrate smoke and intrusion alarms to better manage movement at the campus. By opting to invest in an open architecture unified access control security system, the University of Hull was able to achieve all its security goals while keeping costs low and enhancing the campus experience overall.

WHEN PICKING A SYSTEM, A MAJOR FACTOR IS HOW WELL IT PLAYS WITH OTHER SECURITY SYSTEMS

Unification means, in simple terms, that all physical security components are not only run from the same user component but are, essentially, the same system. When used in a campus setting, the solution can maximise usage of the security infrastructure in place and thereby rationalise the investment. It makes updates seamless and provides a comprehensive cyber security management platform – but also introduces a fresh set of challenges. Technological advances have allowed us to take security to a new level, but today's digital age has also brought to life a new threat: cyber criminals.

Cyber security is also an often-overlooked aspect in campus environments, especially when referring to connected security systems. We've witnessed a significant increase in hacking and cyber attacks in most industries, not least the educational sector. With more sophisticated methods than ever before, cyber criminals are able to use the physical security equipment as a potential entry point to the campus network. A poorly secured camera, unencrypted communications between a server and client application or out-of-date software can all easily be exploited by cyber criminals. Ransomware attacks are particularly costly, and have been known to target educational institutions in particular due to the sensitive data they hold. Most physical security solutions are a work in progress with new devices being added to expand the system or to replace outdated or broken

Picture credit: Genetec

products. The process of adding new equipment – perhaps from a different manufacturer with different security standards – is another opportunity for a vulnerability. No access control provider will be able to perfect a product that has no vulnerabilities, but they should have solid protection in place as well as a process that quickly and completely addresses any vulnerability.

FIRST RESPONDERS MUST GET THE RIGHT INFORMATION TO ACT QUICKLY AND EFFECTIVELY

Due to often tight budgets, educational institutions may be reluctant to transform their security systems. When selecting an appropriate solution, a deciding factor should be how well the new solution plays with other systems. Today, the access control industry is moving away from closed, proprietary systems where only specific hardware is compatible with the chosen software. Instead, we are increasingly moving towards open architecture, where the latest software can be installed to existing hardware, enabling upgrades to be made as needed – without having to sacrifice existing hardware investments. This infrastructure allows for flexibility in choosing systems and the ability to upgrade both software and hardware as needed with time, and according to budgetary restrictions. By supporting the ever-growing collection of open architecture access control modules, readers, controllers and electronic locks, an open-platform access control system futureproofs the investment.

Educational institutions are responsible for creating positive learning environments. Advances in technology have resulted in unified campus security solutions that can deliver comprehensive video surveillance, access control and related functions that not only maximise security, but also offer a multitude of additional benefits. Because administration and security are tasked with protecting students, staff and visitors – usually on a strict budget – it's imperative that campuses invest in a security system that supports this effort today, but is also adaptable for the security challenges of tomorrow ●

Dan Meyrick is Sales & Business Development Manager at Genetec. He has 20 years of experience in the physical security industry, focused predominately on open-architecture security software platforms, products and solutions.

A unified system allows those in charge of safety to monitor the entire campus without needing to hop from system to system

Picture credit: Genetec