Classroom Instructional Technology: Options For Securing Equipment

Charles David Skipton, (E-mail: cskipton@ut.edu), University of Tampa
Erika Matulich, (E-mail: ematulich@ut.edu), University of Tampa

Abstract

University budgets are shifting from the purchase of new classroom instructional technology to the security of existing technology. This paper examines security alternatives, the implications, and challenges of implementation.

INTRODUCTION

Instructional technology in the classroom has become a necessity across many university campuses as the learning environment has turned into a collaborative and interactive experience assisted by technology. According to Quality Education Data, expenditures on classroom technology reached approximately $5.8 billion in the 2003-2004 academic year (McIntire 2004). Despite this astronomical number, instructional technology budgets have been cut at many institutions, with security budgets taking on an increasingly important role (Foster, 2003).

Theft of instructional technology is on the rise (Campus Crime Report Online), and universities are not the only target. High schools, businesses, and colleges from Canada to South America are dealing with the problem. Universities are, by nature, communal environments, and there is exposure of the equipment to various people who come from the surrounding community.

This paper explores security options for protecting instructional technology in the classroom. The experiences of The University of Tampa, a small, private university in Florida, are used as a basis for assessing the security alternatives and options. Additionally, the challenges of costs, implementation, and cultural acceptance are explored.

WHAT IS INSTRUCTIONAL TECHNOLOGY?

There are many forms of classroom instructional technology, all of which add technology hardware and software to the classroom to improve the teaching and learning environment. This equipment could include, but is not limited to, instructor computers, internet connectivity (either wireless or hard wired), student computers (desktops, laptops, or handheld PDAs), video projection to large screen, sound system capabilities, and VCR/DVD players. Other equipment could include digital white boards, document projectors, input tablets, interactive touch screens, and webcams.

All this equipment also needs support, not only from associated software, but also from network technologies, audio-visual maintenance of bulbs, screens, and information technology assistance. Faculty and students may also require training support. Finally, in order to protect the resources installed in the classroom, security measures are required. Finally, these various measures of support may require a complex set of coordinated resources from multiple institutional departments.

A CASE FOR INSTRUCTIONAL TECHNOLOGY SECURITY

The University of Tampa is a small, private university located in central Florida with about 4,500 students and 150 faculty members. Each year, more classrooms are equipped with instructional technology, which usually includes a computer hookup to display from a projector to a large screen, as well as a VCR and sound system. Individual faculty members are each equipped with laptops that they use in their individual offices and bring to the shared classroom space. Some classrooms are equipped with additional technology such as electronic whiteboards or document projection systems. As the technology has been added to the campus piece-by-piece, it has also been disappearing piece-by-piece. In a recent, single academic year, 55 laptops and 32 projection systems were stolen from classrooms and offices. The individual replacement cost of each item did not exceed the insurance deductible, so no insurance claims could be filed. However, the total cost of losses exceeded a half million dollars – a budget amount the small university found difficult to swallow. In the past, proposals for enhanced instructional technology security have been passed over because of the magnitude of the upfront expense, but it became clear that the expense of this security would be far less than the losses from the equipment. Additionally, losses were more than financial – the loss of data, faculty productivity, and student use of classroom technologies was an intangible loss. The University of Tampa faced the challenge of searching for alternative security solutions that would best protect their instructional technology.

SOLUTIONS FOR SECURING INSTRUCTIONAL TECHNOLOGY

After a period of over a year, during which time individual administrative units within the university struggled independently to temper the pace of the loss, a task force of faculty and senior staff was assembled to address the long-term protection of the University's instructional technologies. At risk was not only the potential to lose further instructional capital but the threat that, eventually, one of the technology resources pilfered would contain private or sensitive student information. This potential for a dramatic escalation of losses served to galvanize the belief that the University needed to act quickly. Together, the dean of students, chief university architect, chief of public security, the head of maintenance, head of support services (which includes the janitorial staff and food service employees), deans of the two colleges, head of network services, head of audio video support, and a handful of other key staff and selected faculty from related faculty committees developed the series of potential solutions outlined in this paper.

Solutions for securing instructional technology can be broken down into three basic areas: harnessing, monitoring, and access control. Each of these three potential solutions has its particular costs (which include hardware, installation, maintenance, manageability, and support) and benefits.

HARNESSING SOLUTIONS

Harnessing type solutions include the use of securing cable hardware, hardened steel cages employed as in-class / in-office safes, warbling devices (audio incapacitators and alarms), and should mention of the 'in-house' use of reinforced steel saddles with hardened steel cabling and / or proprietary screws and fastening bolts.

Securing cable hardware. The most famous of the harnessing-type solutions is the Kensington lock which attaches a hardened steel cable to a standardized eighth-inch securing slot included by most manufacturers on the side of laptops, desktop PCs, LCD projectors, and most other electronic equipment. Kensington locks (and devices very similar to them) have been standard issue in the corporate workplace for at least the last ten years.

Outside of the reality that the gauge of cables distributed with the popular Kensington securing system can be cut without too much trouble, the fact is that the variety of unique keys for these securing devices is woefully inadequate. Further, the locks themselves can be disengaged with a steady hand and an unwound paper-clip or, with the aid of a flat-tip screwdriver and a little elbow grease, literally pried from the slot attaching them to the device (this is because the built-in security slots typically provided by manufactures are located in simple hardened plastic housings). While there are ways to enhance a Kensington-type system with the use of large adhesive steel plates

(attached to the secured device) or through the use of heavier cabling (as with the Qualtec securing system) it is clear that Kensington-type systems are primarily designed to serve as a deterrent for crimes of opportunity.

As for the costs of this potential solution, Kensington-type systems are relatively inexpensive to acquire, typically costing between forty and one hundred dollars a unit. If a fastening point is provided in the device to be secured and if the device is located near a large piece of furniture, then installation of a Kensington-type solution requires only the hardware included in the standard bundled kit. The use of additional commercial adhesive fastening points on the secured hardware may require some downtime for the device. Additionally, if needed, the positioning of hardened (and convenient) securing points near where the device is to be located may require the installation of commercial adhesive steel plates to the wall, floor, or furniture or even the installation of I-bolts into the concrete floor or proximal wall. There is no expected maintenance cost for this type security solution and the institutional manageability issues are non-existent as the implementation of the device typically becomes the responsibility of the end user of the secured property.

In-class / in-office safes. A second harnessing solution employs the use of large *steel cages*, reminiscent of the great inquisition, to encapsulate instructional technology – in particular, ceiling mounted computer projectors. While caging valuable instructional technology within a steel box which is then fastened to a hardened steel pole physically secured to the ceiling seems a fair deterrent against theft for all but the most determined thief, it does emote a distinctly negative aesthetic. Further, heavy steel cages have specific architectural requirements for the space in which they are located and, more specifically, for the walls and ceilings to which they are to be attached. Caging solutions also depend on the use of secure padlocks (and necessary secure key systems) to close them.

While caging solutions are only modestly expensive to acquire and install, they are inexpensive to maintain and manage. The cages themselves run from a few hundred dollars to a few thousand and require hardened installation from the ceiling or the wall near which they are positioned. Access to the unit encapsulated in the steel cage for service (like the replacement of bulbs, tightening of cabling, or adjustment of controls) need not be an issue if the cage is chosen carefully to include large and appropriately positioned open "pass-through" spaces for both interaction with the device and its projection out of the cage. If the cage is chosen such that access is only required for installation and heavy service, then a secured key system (with a finite number of known users) does not represent a large manageability cost. There are no unique maintenance or service requirements for caging solutions.

Another harnessing security option is the implementation of in-office/in-classroom *safes*. These enclosures can resemble the caging solutions described for ceiling mounted projectors discussed above but are installed, instead, at floor level. These solutions can include removable shelves and are intended for regular access by approved users to secure portable projectors, laptops, licensed software, data, or other materials. These steel enclosures are typically bolted to either the floor or proximal wall and secured (closed) using heavy steel locks which are controlled via a secure key system (deployed by the institution).

While these floor-level security cages or safes are also only modestly expensive to acquire and install, and while they also have non-existent maintenance costs, they do require a secure system of keys for the users who are approved for access to the secured space. The varied devices range in cost between a few hundred dollars to a few thousand dollars and also require fastening to the floor or wall in a hardened means. Unlike projector cages, in-office/in-classroom safes require regular access and, as such, will require a system of secure keys. The larger the number of potential users who must have access, the larger the potential manageability cost. At the end of the access control section of this paper, the in-office/in-classroom safe solution is amended to include a smart-lock which can give an audit trail of who opened the space, on what day, and for how long. Without such an *intelligent* lock, the manageability costs for this sort of solution depends on the extent of the list of potential users responsible for the secured space and the degree to which a culture of personal accountability has been successfully adopted by the institution.

Warbling devices. Warblers, or "screamers," are audio incapacitators or general alarms used to disorient the would-be thieves with a very loud (>120 decibels) noise while, at the same time, attracting the attention of security. Such devices are either based on mercury switches (movement triggered) or are primed to make noise

when a cable fastening the device to the surrounding space is severed. Potentially, the combination of earlier notification for security and the slowed activity of the thief would result in the arrival of security to forestall the complete removal of fastened devices.

Warblers are relatively inexpensive to acquire, typically costing less than a hundred dollars each, and may be attached to instructional technology devices using steel plates and professional-grade adhesive. Power for these devices typically comes from a battery pack which must be changed according to a regular maintenance schedule. An additional cost that must be considered is the inadvertent triggering of these alarms during normal operations. It would not be unexpected for a legitimate operator to attempt to manipulate projector controls to fine tune its focus or aim. For this reason, the use of mercury switches is not advised unless the device is physically out of reach. Though manageability costs are non-existent, and support costs are limited with an audio alarm solution, regular maintenance of the power source does require some diversion of resources and a period of open accessibility (planned inactivity) for the system of secured devices for such maintenance.

In-house solutions. There are a few other in-house type harnessing solutions for ceiling mounted projectors in particular which focus on the means by which the projector is fastened to a steel saddle, which is then attached to a steel pole, which is then attached to the ceiling. The focus of such solutions is to employ either significantly thicker hardened steel cables or non-standard (proprietary) screws/bolts (where the heads require a particular tool to loosen). Though these solutions represent a great deterrent for crimes of opportunity, they do not serve to protect the instructional device against those most determined to acquire these expensive assets. Experience has shown that, given a sufficient amount of time, steel cables may be meticulously sawed through and the proprietary security screws/bolts have matching loosening devices easily acquired at the local hardware store or via internet. Further, even if careful attention is taken to attach the pole to the device in a uniquely confounding fashion, even more attention must be paid to how the pole is attached to the ceiling. Stories abound of educational institutions having found ceiling mounted projectors taken with their innovatively designed steel saddles and proprietary fastened poles still attached to them.

MONITORING SOLUTIONS:

Monitoring solutions include the use of cameras, RF tagging & tracking, and IP monitoring.

Cameras. The efficient use of *cameras* to limit the loss of assets in the workplace is certainly a complex issue. In this paper the topic will be addressed only briefly and in a fashion that will keep it parallel with the presentation of the other security options. Closed circuit camera systems are expensive to acquire, install, maintain, and support. Individual cameras require power, regular alignment, storage (of captured footage), archiving (long-term storage of captured footage), and active monitoring by support personnel who do not already have functional responsibilities. To complicate things further, complete coverage (even with limited systems that concentrate on all entries and exits) may encounter architectural requirements which increase the cost of their employ and, in some environments, and there are aesthetic complications to be considered (especially in professional and/or historical environments).

Although there are many strategies as to where to place monitoring assets like cameras, a minimum coverage should be applied to *pinch-points* through which all traffic must funnel to enter/exit the facility. Further, there are at least two types of basic strategies when using video surveillance: active monitoring and passive review. If active monitoring is not the objective (or need), then the support costs of video surveillance can be substantively reduced as the need for constant monitoring is transformed into a need for review upon the occasion of an event (passive monitoring). Passive monitoring can be further enhanced when tied to access control technologies (described below) and/or the use of RF (radio frequency) tracking devices.

RF tagging and tracking. Radio frequency tags (RF tags) are extremely small, un-powered, and inexpensive. After a valuable asset is *tagged* (typically with a small self-adhesive sticker) RF monitoring devices (installed in walls or doorways) can detect and log the passage of the tag (attached to the asset) when it passes by. When you tie a video surveillance unit to an RF monitoring device and set it to activate when a sensitive or valuable

asset with a RF tag attached to it a passes by then, potentially, you are able to get a picture (or video) of all persons in the proximity of the RF sensor when the instructional technology left the premises (or left the area in which it was stored). These RF tags are small and can be hidden within an asset (out of sight). Further, as every RF tag has its own unique ID, a networked system of RF monitoring devices could identify when a particular asset was last seen within the institution and, upon passive review of the relevant surveillance media, identify those individuals who could have been in possession of the asset at the time it passed by the sensor.

Though RF tags are inexpensive, the monitoring devices are not especially so. Further, even if RF monitoring stations are installed only at pinch-points and/or all exits to a facility, the numbers of these places can be significant (especially in older structures). Monitoring stations require installation, power, and, if passive monitoring is employed, must be tied to a video monitoring device to be useful. If the assets tagged are limited to those which were assumed to be fixed or if there are time periods during which no tagged assets are assumed to me moved (say after midnight and before 5 AM) then one option would be to set an alarm to sound if any instructional technology passed by an RF monitoring station without prior notification of the monitoring authority. Active monitoring of assets, an extreme possibility for an employer, would require additional support personnel. Manageability requirements for RF tracking with anything other than passive monitoring have the potential of becoming a significant consideration as permissions for movement must be maintained and coordinated between the relevant, responsible parties.

IP monitoring. It is possible to monitor the presence of instructional technology using the computer network to which many of devices attach. Every device attached to an institution's computer network has a unique network interface device which it uses to communicate with the network. Servers attached to the network can be tasked with *pinging* (or electronically shaking hands with) each piece of instructional technology attached to it every few seconds. This process is called *IP monitoring* (every device on the network has a unique internet address, a so-called IP). When a device unexpectedly leaves the network, for whatever reason, it can signal an alarm which then can notify security personnel that there is a problem.

IP monitoring can work well for pieces of instructional technology that are both permanently attached and powered on, but will not function for devices that are either *completely* powered down at some point or for assets that physically leave the network at night (like laptop computers) without the use of special auxillary hardware monitors (described below).[1] Still, if the policy within the institution is to report the temporary powering down of a device like a projector or the physical removal of a personal computer from the network to the monitoring authority before such an event, for whatever reason (perhaps to replace a bulb on a projector or relocate a PC), then ordinary IP monitoring can function well within standard educational institutions.

Though most modern IT devices already posses network interface devices within them, some are not "always on." Instructional technology devices that fall into this category would require the addition of an auxiliary monitoring device to attach to it which has within it a network interface device that is "always on." Installation of such IP signally devices is typically not especially costly but the devices themselves (which can often monitor multiple, proximal, physical devices) can cost a few hundred dollars each.

IP monitoring requires a server to monitor the presence of the instructional technology and any IP reporting devices found within the network. These duties may be fulfilled by current server assets but represents an additional potential costs for some institutions. Further, while most modern PCs and networked peripherals would not require additional hardware assets to be monitored on the network, devices that are completely powered down at night or which do not possess a network interface device may require the acquisition of the auxiliary IP monitoring devices describe above. Though typical maintenance expectations are limited, expected support and manageability responsibilities are potentially extensive. Instructional technology, when limited to computer projectors, can be expected to remain in one place most of the time (except when the projector is under maintenance). Instructional technology when expanded to include PCs, laptops, and other peripherals (especially if the use of mobile units is

[1] When the power on a modern personal computer is shut off, while it remains plugged into the wall, a limited amount of power is typically channeled through the network interface device within the computer. So, on such devices the powering down of the PC will not hinder a server on the network from pinging it. This is not the case with most computer projectors (or other potentially valuable instructional peripherals).

employed) should be expected to move about on a regular basis. If the second, broader, definition of monitored instructional technology is employed, then the coordination of the varied assets on the network increases costs and can require additional staffing resources.

ACCESS CONTROL

Access control solutions, broadly defined, include the use of steel keys, punch-key & key-pad locks, smart keys, and traditional card access. These solutions may be further divided into access control solutions with audit trail capabilities and those without. Additionally, within these two broad categories there is a distinction between those without the capacity to be monitored, those that allow for active monitoring and those that allow only for passive review.

An *audit trail* is a formal record of every user who gained access to a particular controlled space at a particular time. Though there are administrative procedures that can be followed to track who had access to particular traditional steel keys at particular times and/or who may have been originally issued a numeric key-code, steel keys and punch locks/pads do not have the capacity to record who entered what space and at what time, and so, are not considered access control technologies in the formal sense.[2] Regardless, a discussion of the use of steel keys and punch keys/locks would be prudent in this analysis as they are in wide application today.

Active monitoring systems are those which allow real-time information to be reported to a central location regarding who has entered what space and when, whether or not a particular door is open or not, and the current level of the power unit employed within the access control system at that location. The defining difference between *stand-alone* devices (those that do not allow for active monitoring) and systems that allow for active-monitoring centers around whether or not the device is connected to a central server over a network. Some smart-key and card-access systems can be networked and, so, allow for active monitoring. Networked access control systems are also called *hard-wired*.

One last defining characteristic among access control systems relates to whether or not the power for the system (assuming it is not purely mechanical like steel keys and punch locks) is provided via a battery pack or via a wired power connection. Access control systems that are physically connected to a central power source are also called *hard-powered*.

Steel keys. 'Steel keys' refers to any system of traditional locks which are manually powered and which use blank key-stock that may or may not be proprietary to a particular maker. Some steel key solutions employ non-traditional blanks that are proprietary to a particular firm – they may even employ patented key blanks. The result is a key that is very difficult to copy – though blanks for even the most proprietary systems have a way of finding their way to markets for those who are interested enough to search for them. From an access control standpoint, keys for a particular lock can be assigned to a finite list of persons. Thus, determining who entered what space is simply a matter of looking up who had a key issued to them for that time. Although sub-master and super-master keys are often employed for steel key systems, their numbers are typically limited.

Steel key locks typically range in cost from forty to one hundred dollars per door, before installation, and require limited maintenance for their prolonged use. Steel key solutions can be found for most any door medium whether glass, solid wood, or hollow door. Further, steel key locks are weather resistant and operate in all lighting environments (something not universal among access control devices). Manageability and support costs for steel key systems escalate with the number of doors and according to the complexity of the institutional structure. A secure system of keys requires a clear system of rules, an ingrained culture of individual responsibility, and a level of staffing which allows for the collection and destruction of old steel keys and/or the identification of devices that must be replaced (or re-keyed) due to the misallocation of a key or master-key.

[2] While some electronic punch code locks can maintain an audit trail of which codes were used to open which locks at which times, codes are easily duplicated; therefore there is no way to be sure who actually punched the number into the lock.

Punch-key and key-pad locks. Punch-key and key-pad devices are combination entry devices. Some of these devices, when electronic (key-pad), may have limited audit trail capacity recording which code entered the lock at what time and on which day. Mechanical (punch-key) devices do not have this capacity. These devices are very similar (in function) to the steel key locks which they replace with one exception – the blanks for the lock are costless and the ease of the user to duplicate the combination-code key is limited only by the institutional rules (and penalties that apply) for its duplication. Unlike the steel key devices that they replace, most of these access control devices are somewhat large (with the electronic variant either requiring space for a battery pack or for the installation of a direct connection to live current). This sort of access control device is well suited for perimeter control needs where many different users are to be given general access and where there is no real need exists to track which individuals had access to a particular space at a specific time.

Punch-key and key-pad devices can vary in price from a few hundred dollars for mechanical punch-key locks to three or four-hundred dollars for stand-alone, non-hard-powered punchlock systems. Installation is similar to that of steel-key solutions with the exception of the hard-wired and / or hard-powered punch-key solutions. Punch-key solutions are mechanical and, so , require maintenance in the form of annual grease treatments – a requirement which can necessitate additional support personnel (depending on the size of the access control system). From a manageability perspective, the cost of administering a punch-key / key-pad solution increases at a greater than linear rate with the number of users and according to the complexity of the organization (similar, in effect, to that of steel key solutions).

There are a few hybrid steel-key and punch-key / key-pad lock systems that require the use of a punch-code to release access to a steel key lock which is then ultimately used to open the lock. Such systems are more accountable than punch-key/lock solutions (as the duplication of steel keys is never costless – especially when proprietary key blanks are employed).

Smart-keys. A smart-key is a mechanical key with a computer imbedded within it which communicates with a smart-lock containing a data-base of allowable smart-keys for that lock. Each key has a unique ID which cannot be altered or duplicated. Smart-key solutions (like Intelli-key) allow an administrator to turn a particular lock "on" for a particular key, a series of locks "on" for a particular key, turn "on" a particular key for a set of specific locks for particular times, to set a key to expire (negating the need to retrieve keys from departed personnel or even adjuncts that only work every few terms), turn a particular lock "off" for a particular key, turn a set of locks "off" for a particular key, or even set a lock to open/close automatically at particular times on particular days during the term (so called 'time-zones." The use of time-zones eliminates the need to issue any keys for those scheduled to use a controlled space at times the door is scheduled to be open, which makes access by adjunct faculty, graduate students, staff, and undergraduates much easier. Further, smart-key solutions log the entry and attempted use of all keys in each device on the system. One potential drawback of many of the smart-key technologies is that many of them (including Intelli-key) use IR (infra-red) transmissions to communicate between the key and the lock, and so, implementation where there are periods of intense and direct sunlight can, on occasion, play havoc with the technology. This hybrid mechanical – electronic lock system is also not sealed to the elements (as the key has to be physically inserted into the lock) – increasing the cost of maintaining such locks in particularly damp or humid environments. Real-time monitoring is possible for hard-wired smart-key solutions, but most are built to be stand-alone devices.

Smart-key solutions range in cost from three hundred and fifty to six hundred and fifty dollars per lock. Installation costs are similar to those of punch-key/key-pad solutions in that they require a bit more space for their battery packs and computer parts. Hard-wiring and/or hard-powering smart-key solutions can similarly increase installation costs to almost fifteen hundred dollars a unit. From a maintenance cost perspective there are two additional costs to the use of these hybrid electric/mechanical devices: necessary annual lubrication and a maintenance schedule (typically annual, but less frequent for doors without significant traffic) for the replacement of batteries within the stand-alone systems. Smart-keys themselves cost approximately twenty dollars each, which is more expensive than regular steel blanks. Manageability of a smart-key solution can be done at a micro (administrative unit) level or at a centralized level of bureaucracy. While centralized control of a keying system has its cost advantages, the information available for controllers at a more local level allows for administrators to easily

turn locks on and off for employees who leave, whose needs change, or whose particular needs are complicated and / or intermittent. Centralized control would require additional support resources (in the form of additional personnel) while the use of limited, local zones of control requires only modest human resource commitments.

Smart-cards. Smart-card solutions employ a card with either a microchip or RF chip imbedded within it. One advantage to this potential solution is that many educational institutions already employ a smart card technology distributed to all students and employees in the form of their ID card (typically used for food plans, sporting event tickets, library services, medical services, etc.). If so, the purchase and distribution of new *keys* is not necessary. Smart-card solutions should not be confused with other traditional card-access systems that use a magnetic strip along the backside of the card that may either wear with mechanical use, deteriorate with exposure to the sun, or be copied through the use of easily acquired magnetic stripe encoders in the marketplace. As many smart card solutions use RF tokens as well as smart chips, they often function as proximity readers (meaning you have to wave the card near the lock instead of having to insert it into or pass it through the lock). As such, there are very few parts in the reading part of the device that are mechanical (unlike with smart-keys). Non-RF readers use a slot reading system, similar to those used with traditional magnetic stripe readers, and are also not as subject to mechanical wear as with smart-key mechanical systems. As far as functionality goes, the smart-card access control devices function identically to that of the smart-key technologies.

Smart-card solutions range in cost from six hundred and fifty dollars to eight hundred and fifty dollars each. Hard-wired and hard-powered solutions can increase the hardware and installation totals to nearly fifteen hundred dollars per door. Active monitoring, in hard-wired, hard-powered systems, is possible. Installation and manageability costs are identical to those with smart-key solutions. However, as there are not as many moving (mechanical) parts to the lock the maintenance and related support needs (for the maintenance needs) are reduced.

HYBRID SYSTEMS AND THE ABUNDANCE OF INFORMATION

One strategy for securing a learning environment, and the instructional technology that exists within it, is to provide one of the potential solutions described above especially well. A second, significantly more powerful solution, though, integrates solutions of the list from above together into a *system* best suited for the institutional environment in which it exists. Consider the theft of a piece of instructional technology from a secured facility employing a system of access control and video surveillance. It is one thing to have a record of an individual's unique ID opening a secured door (behind which the stolen instruction technology was located). It is something else entirely different to have video of the individual on the premises around the same time (eliminating the possibility that someone used his unique university credential without his knowledge or permission). Alternatively, consider the use of RF tags tied with video surveillance technology which captures the image of any person transporting any tagged device through monitored space (like entry/exit pinch-points). Each of these integrated solutions represent a non-linear increase in the power of individual security solutions outlined and categorized above. Another hybrid solution employs both a harnessing solution and an access control device in the form of an access-control locker. By using either a smart-key or smart-card access control lock with a in-classroom / in-office safe used to store instructional technology for shared resources seamlessly integrates the harnessing benefits of an in-class safe with the personal responsibility aspects of an access control technology capable of producing an audit trail of those users who opened (or attempted to open) the secure instructional technology storage area. The range of integrated possibilities is extensive, and while integrating solutions increases all aspects of cost identified in this paper (hardware, installation, maintenance, manageability, and support), *the* abundance of information it creates actually serves to limit the threat of theft exponentially.

There are many other potential solutions to securing of instructional technology in university/college environment. Notably absent from the discussion above are the following: the use of monitored, professional, alarm systems such as Brinks; the use of "call home" software / hardware which is installed / soldered into instructional technology equipment and programmed to contact authorities if and when it realizes it has left its "home domain;" and the use of centralized secure rooms (access-controlled storage centers for instructional technology). The sections above outline the leading topics within the market for the securing of instructional technology within open access facilities (as opposed to closed work environments like bank offices, administrative offices for private firms, and

government office buildings). The problem of securing information technology within these environments is equally as challenging but allows for a different set of optimal solutions.

ORGANIZATIONAL AND CULTURAL IMPLICATIONS OF SECURING INSTRUCTIONAL TECHNOLOGY

Security devices for instructional technology are arguably important, but the procurement and installation of such security is fraught with challenges. Of course, the first is budgetary concerns. All the security solutions mentioned in the previous section have associated hard and soft costs. Typically, educational institutions have fixed budgets set a year or more in advance, so even if new instructional technology equipment was budgeted for, the additional costs of securing that technology may not have been part of the budget request.

Another part of the challenge of securing instructional technology is that this new budget item spans many areas of responsibility. For example, at the University of Tampa (as mentioned above), multiple departments had to be involved in designing solutions simply for securing projection systems in the classrooms. The Audio Visual department is responsible for projection systems, so security devices had to be evaluated in terms of their compatibility with existing projection systems. The Information Technology department had to be involved when network connections and IP addresses were required for hooking up the projectors. The Chief University Architect had to assess the structural integrity of the rooms in which the various solutions were being considered. Facilities was responsible for hard installation of the security "cages" around the projectors. Campus security, who would be notified if a security breach took place, also had to be involved. The Dean of Students had to assess how students were impacted by the access restrictions imposed by the new security technology. Faculty committees concerned with instructional technology were also involved so they could clearly communicate any changes with instructional technology's end users. The ultimate question became…whose budget would this security expense come out of? IT? AV? Security? Facilities?

There are also legal implications for some security technologies. Studies have found an increase in people feeling safe in areas with surveillance, followed by a decrease in actual crime levels (Fry, 2004, p. 6). However, several concerns have been raised about this technology. Courts have had to analyze the use of such surveillance in two distinct areas. First, courts have looked at the necessity of using such technology to take reasonable measures to deter criminal activity on their property. Second, the courts have looked at issues surrounding the invasion of privacy from the technology. The use of the technology must follow limits established by the constitution and laws along with protocols of ethics and professionalism that prevent "unreasonable intrusion into the privacy rights of individuals" (Bickel and Brinkley, 2004, p. 303). Video technology can legally be used only to enhance existing security measures, but not replace the use of security guards to save money. Strict standards regarding the location of the cameras and the use of the tapes must also be followed (Bickel and Brinkley 2004).

Organizational culture issues are a challenge. Faculty members might not feel it is "their job" to deal with security issues. A culture of personal responsibility must be endorsed by upper-level management (e.g. department chairs and deans). Classroom technology and security solutions must also be accompanied by faculty development (Plotnick 2004). Without knowledge and training, faculty are far less likely to use instructional technology or care about securing it. Organizational culture, as it relates to responsible actions regarding the security of instructional technology, is an area of research that will be addressed in the future work by the authors of this paper and is an area of incredible importance and complexity.

CONCLUSIONS

Public and commercial pressures for innovation push organizations to continue to add and employ the latest technology. But college and university campuses provide a unique open-access environment in which it is especially challenging to secure this highly valuable and, at the same time, highly portable instructional technology. The management structures of colleges and universities are typically not designed to keep pace with the rapid changes that occur in the high-tech part of the instructional technology sector. For starters, they don't have a direct financial incentive to develop both a timely and efficient management of the technology and they lack the flexibility to facilitate the timely transfer of internal funding for the optimal level of investment. Security measures are often

ignored in the drive to place technology in the classrooms because security issues challenge organizations across multiple departments and administrative entities. The adoption of instructional technologies should have security implications as part-and-parcel of the budget, installation, and subsequent training.

We currently see how technology is fundamentally changing education, making the classroom more student-centered and learning more student-driven. Yet, the challenge for leaders is not only about recognizing the benefits technology provides, it is also about leading others to see technology's potential and promise, discovering funding for its implementation in typically tight or shrinking budgets, and protecting the technology once it is finally acquired (Golden 2004). Ultimately, the challenge is about helping all stakeholders use technology to transform the culture of education to enhance student performance

REFERENCES

1. Bear, Charlie, Head of Physical Plant, The University of North Florida; Implementer of access control technology (smart-key technology) for the past 9 years. Interview conducted September, 2004.
2. Bickel & L. Brinkley, (2004). "Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or will the Courts Strike a Proper Balance?" *Stetson University College of Law 25th Annual Law and Higher Education Conference Manual*. Clearwater Beach, FL. February, pp. 301-316.
3. Golden, Michael (2004), "Technology's Potential, Promise for Enhancing Student Learning," *T.H.E. Journal.* Jul y, Vol.31, No. 12; p. 42
4. Campus Crime Report Online. "Campus Crime Report." http://ut.edu/directory/administration/ crp2000.html
5. Foster, Andrea L. (2003), "Technology: Less for Computer Systems but More for Security," *Chronicle of Higher Education*, December 19, p. 11.
6. Fry. (2004). "CCTV Public Area Surveillance in the UK, Why Have a CCTV User Group?" Stetson University College of Law 25th Annual Law and Higher Education Conference Manual. February, p. 6.
7. McIntire, Todd (2004), "Enough to Go Around?" *Technology & Learning*, April 1, p. 32.
8. Plotnick, Eric (2004), "Educational Technology, Research and Development," *Instructional Technology, Washington*: Vol.52, No. 2; p. 108.
9. Porter, John, Information Systems Security Consultant. Interview conducted October 2004.
10. Stone, DeWayne, Locksmith, Rollins College (FL). Implementer of access control technology (smart key devices) first at the University of North Florida, then at the Orlando International Airport, and now heading a conversion to access control at Rollins College. Interview conducted September, 2004.
11. Vahle, Kurt, Security Manager, Shands Hospital (The University of Florida). Implementer of various access control technologies (including stand-alone and hard-wired smart-key and smart-card systems) for the last 8 years. Interview conducted September, 2004.