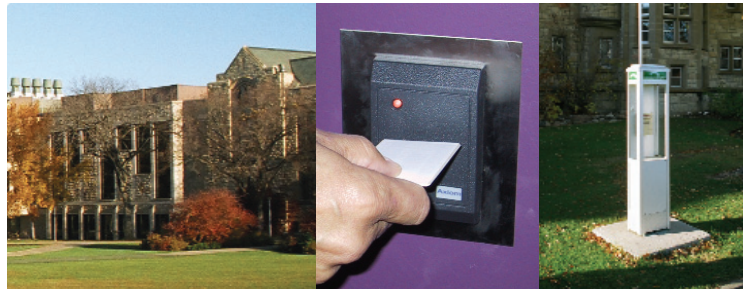


The logo for delcosecurity features the word "delcosecurity" in a bold, blue, sans-serif font. To the right of the text is a graphic consisting of a blue sphere at the top, with three white curved lines that sweep downwards and to the right, suggesting motion or a network.

## INTEGRATED SECURITY SYSTEMS

### APPLICATION NOTE — UNIVERSITIES

#### Summary

A university's security environment is similar to that of most large enterprises today. A university's assets are located in many separate buildings, usually in a campus setting, but sometimes located beyond the confines of the campus. Universities, offer a greater security challenge than corporations. Universities are required to provide easy, open access to the public. Their populations, especially students, have a very high annual turnover.

A very large component of a university's assets is its intellectual property which is stored and managed on its computer network. There is a growing trend in the security industry to bring together the physical security environment and the cyber security environment into a single security framework. This is becoming especially important to universities. We see universities taking an active role in both the development and implementation of this emerging security technology.

#### University Security Needs

Security at a university covers a wide range of needs.

Valuable physical assets of laboratories, art galleries and museums, etc. are dispersed across the campus and beyond.

Student residences raise other threats of theft and personal protection.

Personal safety on campus and in parking lots, especially at night, needs to be addressed in the campus security plan.

A campus security plan will include video surveillance and access control systems to mitigate the above threats.

Universities rely upon, and take for granted, their buildings' infrastructure such as utilities, (light, power, heat, cooling), telecommunications, computer network, and security. A comprehensive university wide security program should provide central monitoring and central command post for integrating video surveillance, access control, and utility monitoring in one overall system based upon an overall security program.

Management of access privileges is a significant administrative effort at universities. Some of the access privileges that need to be managed and controlled are:

1. Physical card access for students in residences
2. Card access to administration offices and laboratories
3. Network Login privileges for undergraduates, and graduate students
4. Administration network login privileges

Significant cost saving and increased security is achievable at universities by planning an overall campus security plan and system which embraces both the physical and cyber access control issues in a common framework.



A second opportunity to lower costs and improve quality is to add access control functions to the "Student Card" that many universities provide for student financial transactions. Again one set of identity validation and privileges management processes can be achieved with this dual purpose card.

*Passionately focused on your success*

## The APEX Solution

DelcoSecurity has over 10 years of security automation experience, and understands the unique needs of universities.

APEX, DelcoSecurity's enterprise solution monitors and controls to all security and building management functions providing security staff with co-ordinated visibility on all activities on campus. With this information security staff can quickly mount an effective response to threat or situation.

APEX is completely based upon IP network topology. All cameras, recorders, access control systems communicate on the university's existing IP LAN/WAN. Almost no special or additional wiring is required.

## Benefits

- Campus wide surveillance, access control, building management monitoring, incident response based upon existing LAN/WAN network.
- Support of multiple control posts receiving information from all security subsystems
- Choice of many access tokens such as cards, fobs, biometrics (fingerprint, hand print, retinal scans etc.)
- Convergence of "student cards" with access control
- Convergence of physical access with computer network access

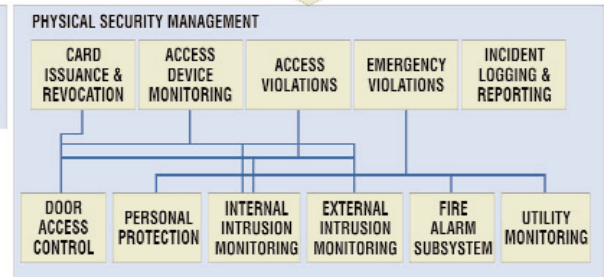
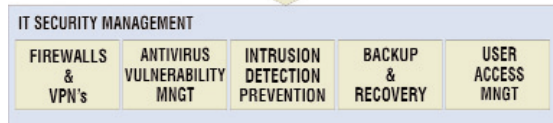
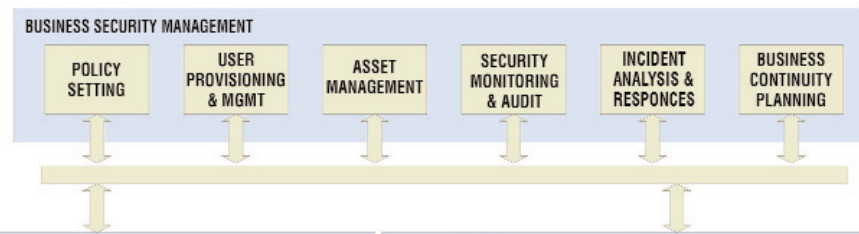


## APEX Business Security Management

The "APEX Business Security Management" option addresses the convergence of physical security and cyber security.

There are strong business imperatives to converge IT security with overlapping physical security. A cornerstone of security is identity management. Identity management consists of validating the individual is who he/she says she is, validating their role in the organization, and assigning access rights and privileges based upon their role.

- Consolidate credentials for IT and physical access onto a single card. Standardizing on a single card may save costs and improve security.
- Connect granting and revoking building access privileges with IT access. When a person's role changes, ( e.g. new hire, promotions, dismissal) it is important their new role is reflected in both their IT access privileges and physical privileges simultaneously.
- Correlate security events across the physical and IT realms. For example, an alarm incident should



trigger if the door access system indicates a person is in a given room, and at the same time she/he is attempting to login remotely.

- Unify the auditing of physical and IT rights and events. By assessing authentication and authorization processes and controls across IT and physical facilities, organizations will find improved efficiencies and security. One business process for identification and assignment of rights for door access and IT is an obvious area of cost reduction and improved security. An audit of current practices in an organization will certainly find others.



[www.delcosecurity.com](http://www.delcosecurity.com)