Physical IT Facilities Security

EDUCAUSE Evolving Technologies Committee
Bonnie Neas, North Dakota State University

Summer 2003

Introduction

Since 9/11, security has become common nomenclature to cover a broad range of issues dealing with the safety within our country. We all know, however, security breaches are not carried out only by terrorists. Intrusion, theft, destruction of property and even human error can create severe disruption of services. In the past two plus years, of most concern to us in higher education’s information technology (IT) environment has been the issue of keeping our networks secure to protect our information.

In 2001, our campus began the process of designing a new building that would house a number of nanoscale science projects and our new Center for High Performance Computing (CHPC). In the early design phase, it was clear that securing the facility was a priority. The engaged architectural firms – both local and from Minneapolis – requested our security requirements. We are fortunate to have a very knowledgeable network services and facilities services staff that were very helpful in developing the requirements for our network security, however, less was known about what should go into securing our building – post 9/11 – to protect our new research and CHPC facilities. In perusing the web, an abundance of information was available about securing our networks and data, but very little information was available about securing our physical facilities. Therefore, this paper attempts to address the less mentioned and less written about yet very strategic and critical – physical IT facilities security.

What is Physical IT Facilities Security?

Physical IT facilities security is protecting our institution’s information technology assets that may be housed in areas such as buildings, rooms, closets, or underground tunnels. As our institutions design new or upgrade existing IT facilities, a high priority must be placed on securing them.

Why Is Physical IT Facilities Security Important to Higher Education?

Protecting our capital assets is important because of the complex networking and server environments universities have and the productivity they enable. All colleges and
universities – independent of size or program complexity – need to be concerned about protecting their physical IT assets. Providing robust, stable IT services has become an essential need for organization's daily operations whether they are in our admissions office, library, research laboratories, classrooms, purchasing office or in a student’s residence hall room.

What Are The Implementation Challenges?

The culture of a university has been and continues to be open and flexible – in support of discovering, creating, maintaining, and/or sharing knowledge. Even though our networks and our physical computer rooms have long seen the need for protection from outside intrusion, 9/11 created additional urgency in addressing this issue. There is very little documentation on how universities have addressed the issue of securing their physical IT facilities. However, one agency has been addressing this issue for years – the U.S. Department of Defense. After careful review, it was noted that many of its requirements could be applied to the higher education environment.

The Department of Defense (DoD) started the process of formalizing the securing its computer assets as early as 1967. Construction requirements include:

– walls from floor to ceiling – preventing crawl space from room to room via drop ceilings,
– doors, wood or metal with locking devices;
– windows that include wire mesh

DoD states how important it is to have well-written policies on who may have access to facilities and who explicitly has responsibility for facilities – (from Department of Defense; DoD 5200.28-STD; Trusted Computer System Evaluation Criteria, December 1985.) Very complete documentation can be found by doing a search at DoD’s Defense Security Service – www.dss.mil. At that site you can do a further search on Construction Requirements – http://www.dss.mil/search-dir/isec/chapter5.htm chapter 5-801.

Another site of interest – www.cybercon.com/tour_security.html – stated a solution that may be relevant to many of our campuses. It suggests four levels of security for physical access that may house sensitive IT equipment or services. They are:

– code access to the building
– biometric access to the floor
– card reader access to the server area
– locked cabinets for security hosted servers

In addition to this access control, its facilities are also monitored by security cameras and 24/7 staff. It is assumed that some of our universities have adopted similar levels of security – if not to entire buildings, perhaps IT space within buildings with other academic
activities.

The SANS Institute Reading Room – [http://www.sans.org/rr/](http://www.sans.org/rr/) – provides an interesting index to many IT security topics. This site provides good reading but it primarily addresses the “soft” security issues of protecting information on the networks versus the “hard” security issues of protecting our physical spaces.

**Who Are The Major Physical IT Facilities Security Vendors?**

Vendors are the architects and engineers who have the knowledge to design new buildings or retrofit existing building resulting in making our networking and computer facilities safer. Our experience demonstrated that except in the large metropolitan communities, few architects and engineers have experienced working with agencies, such as Defense or businesses such as financial institutions or for-profit software development companies such as Oracle, in designing the highest levels of security into facilities.

In surfing the web to research information about this topic, it was discovered that numerous conference agendas for businesses include sessions on securing facilities. Past trends included a large business building in a single corporate complex. Today’s trend is to disperse buildings and resources afar rather than cluster them in a single location. Even though universities have long had off-site facilities to store critical back-up information, it may now make sense to disperse other resources such as servers and not “cluster” critical infrastructure resources.

It is imperative that as new institutional facilities are designed or existing facilities are upgraded, physical IT facilities security requirements become an integral part of the process of hiring knowledgeable architects and engineers. The American Institute of Architects - [www.aia.org](http://www.aia.org) – is a good contact to identify a responsible architectural firm. Also, when hiring, ask for references dealing directly with designing facilities with the security features needed. An expected outcome is that they know a lot more about this issue than you do. [http://www.aia.org](http://www.aia.org).

**How Should We Proceed?**

Continue to discuss the need for good information. There currently is an abundance of good information on how to protect our applications and networks – as an example see [www.educause.edu/security](http://www.educause.edu/security), but there is little, well organized information on what is required to design new buildings or retrofit existing facilities to make them safe. There should be a collection of “best practices” including reliable web sites. This could be a small project undertaken by EDUCAUSE since they already have other security initiatives.
When Will Physical IT Facilities Security Become Essential on Campuses?

Information on good building design that includes proper security for our IT assets is needed now. Those responsible for the safety of their campus’s physical IT facilities should be educated on the issues if they are not already aware. The topic should be included in our conference agendas. Working groups should be formed to create awareness of this issue by collecting examples of best-practices including sound building design and policies that go along with securing our campus facilities.

How Is Physical IT Facilities Security Evolving?

Most conversations still focus on the “soft” issues of IT security, such as keeping our networks and/or desktops secure. These are important issues, however, there appears to be little discussion or little written about the security needs of the physical side of our campuses.

Conclusion

Since 9/11, we live and work in different times. Security is no longer taken for granted. Not only do we have hackers and viruses, but we have many throughout the world who would like to see our productivity halted and our economic assets destroyed. Many of those assets can be found at our university campuses where we have always enjoyed an open atmosphere to teach, to create new knowledge, to learn and to work.

Related Higher Education Projects

EDUCAUSE and Internet2 have a joint task force – the EDUCAUSE/Internet2 Computer and Network Security Task Force. Rodney Peterson provides leadership as it’s Director. For additional information see: [http://www.educause.edu/security/](http://www.educause.edu/security/)

Related EDUCAUSE 2003 Sessions

Three pre-conference seminars on Tuesday, November 4, address aspects of IT security. They are:
- Seminar 12P - “Information Security Risk Evaluation for Colleges and Universities.”

Most security topic sessions can be found daily in Track1. Additional sessions that address security concerns are:

**Wednesday, November 5:**
- Track 7 - “Security Training and Awareness on a Budget.”
- Poster sessions: “Security Awareness and Defense in Depth: Methods for Expanding Security Strategies to Academic Departments” and “Management: Awareness is the Key to Security.”
- Current Issues Roundtable - “IT Security: What’s Our Status Within Higher Education?”

**Thursday, November 6:**
- Track 6 - “IT Security: The State of the Practice in Higher Education”
- Meeting (open) - EDUCAUSE/Internet2 Computer & Network Security Task Force

**Friday, November 7:**
- General Session - “The Academy’s Obligation to Secure Its Cyberspace”

The broad range of security topics include policies, training, organization, network security and information security. However, little is said about building and/or keeping our physical spaces secure.