December 2004

Designing Information Systems Security Policy in Higher Education

Jon Saltzman
Claremont Graduate University

Abhijit Gadkari
Claremont Graduate University

Designing Information Systems Security Policy in Higher Education

Jon Saltzman
School of Information Science
Claremont Graduate University
jon.saltzman@cgu.edu

Abhijit Gadkari
School of Information Science
Claremont Graduate University
abhijit.gadkari@cgu.edu

ABSTRACT

The aim of this paper is to introduce an information systems security (ISS) policy framework for higher education institutions. Discussion on security and academic freedom of expression highlights the challenges involved in design and implementation of a policy model in this environment. Issues of shared governance are explained. These issues demonstrate the need for the Academic Security Visibility Model (ASVM). The ASVM builds on the existing KMPG Security Capabilities Model and other research. Different security scenarios will be explained on the basis of the ASVM. This paper presents a matrix methodology to evaluate infrastructure, resources and activities in the higher-ed environment

Keywords

Academic, security framework, policy, computing, higher education

INTRODUCTION

In higher education institutions, the goal for information systems managers is to provide students, professors, faculty and staff of an institution the ability to freely "share data and collaborate on projects" (Walton, 2002). Inherent to this goal is the idea that the technology used should not interfere with the user's activities. On the other hand, attempting to achieve this goal without proper planning or policy in place may lead to insecurity. Even with proper planning, this goal may be difficult to achieve. Within most academic institutions, the goal is (or should be) to be as secure as possible without limiting "academic freedom" (Roiter, 2001).

It is a challenge to develop security policy at all organizational levels in the academic environment given the diverse needs of students, faculty and staff. While there are corporate models for security, there are few clear models that help the academic organization understand its own needs. What works for a Fortune 100 company may not work for a small liberal arts college, although some of the needs will be similar. Academic institutions often function under the notion of "shared governance" which is in direct contradiction to the top-down, hierarchical approach of many corporations. The academic environment is subject to many unique pressures.

There is also a disjoint, or "gap" between policy and practice. We recognize this need for practical policy, as well as the need for high-level models. To address this problem, we propose the integration of some common security models, those being the KPMG Security Capabilities model and the Security Development System Lifecycle model (SecSDLC). We also propose our own model to help clarify the problem domain, called the Academic Security Visibility Model or ASVM. The ASVM attempts to show the interests of the stakeholders through equal representation, as opposed to a top-down approach.

BACKGROUND MATERIAL

Shared Governance & Academic Freedom

Shared governance is traditionally defined as the involvement of faculty in institutional policy-making (Gerber, 2001). This definition has been slightly updated to include students as well, with students playing a role in organizational decision-making. Essentially, shared governance means equal rights when it comes to how the organization formulates a policy.

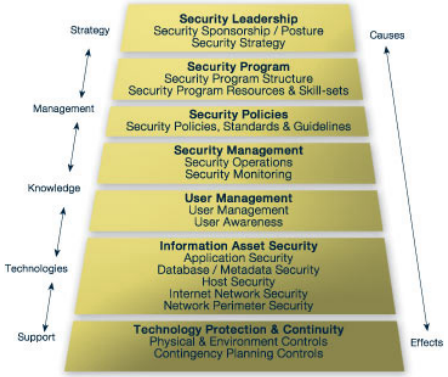
Academic freedom, as defined in the Columbia Encyclopedia, is the "right of scholars to pursue research, to teach, and to publish without control or restraint from the institutions that employ them" (Columbia Encyclopedia, 2001). Academic freedom is a necessity for colleges and universities (Gerber, 2001). It has even been proposed that academic freedom is beyond the scope of the United States Constitution, which protects the freedom of individuals to a high degree (Gerber, 2001).

In general, “a conflict exists between the rights of students and faculty to free speech and privacy, and the obligation of universities, parents, and society to restrict access to information deemed unsuitable for youth” (Peace, 2003). Faculty need the “affirmative authority to shape the environment in which they carry out the responsibilities”, within reason (Gerber, 2001). Faculty must be entitled to freedom in classroom discussions, research and publication of results, and artistic expression (Educause/Internet2 workshop, 2003). In addition, faculty & students should be allowed to “seek, receive and impart information, express themselves freely, and access material regardless of origin, background, or views of those contribution to their creation” (Educause/Internet2 workshop, 2003). Within academic environments, there is much tolerance and experimentation, and anonymity is highly valued (Bruhn & Petersen, 2003).

These requirements of academic freedom are “inextricably linked” (Gerber, 2001) with shared governance. Gerber argues that “shared governance is taking on new importance as a means of trying to preserve the ideals of liberal education that are necessary for the continued vitality of our democratic society” (Gerber, 2001). Clearly, the political model of shared governance is the means by which faculty/students of academic institutions should be able to make their needs visible and preserve their academic freedom.

The KPMG Security Capabilities Model

In 2002, KPMG performed a “Global Information System Security Survey” in which they interviewed 641 senior managers of global business firms by telephone (KPMG website 2002). One of the results of that survey was the KPMG Security Capabilities Model (KPMG website 2002). There is some evidence that academic institutions are aware of this model and are interested in its applications in enterprise-wide information security policies/systems (Walton, 2002). Although originally designed around the business firm, because academicians have shown their interest in this model, it seems important to validate this as a piece of the information systems security and policy puzzle.


Strategy
Management
Knowledge
Technologies
Support
Security Leadership
Security Sponsorship / Posture
Security Strategy
Security Program
Security Program Structure
Security Program Resources & Skill-sets
Security Policies
Security Policies, Standards & Guidelines
Security Management
Security Operations
Security Monitoring
User Management
User Management
User Awareness
Information Asset Security
Application Security
Database / Metadata Security
Host Security
Internet Network Security
Network Perimeter Security
Technology Protection & Continuity
Physical & Environment Controls
Contingency Planning Controls
Causes
Effects

An effective security environment requires comparable capabilities at all levels

Figure 1. Enterprise Security Capabilities Model (KPMG, 2002)

The model clearly breaks each level into one or two problem areas, which are handled by organizational stakeholders in that level’s domain (i.e. the strategic level handles both the leadership and over-arching structure of ISS). In effect this creates somewhat of a “checklist”, which roughly maps to the overall structure of the organization. Each “domain” consists of some security responsibilities, which are stated by title but not defined in any detail (for example, what does network perimeter security *really* entail?).

The largest criticism of the KPMG model is that it says nothing directly about the process of developing security policy. In Planning and Control Systems: A Framework for Analysis (written in 1965), Robert Anthony describes a framework that “consists of formal planning and control *systems*, designed to facilitate planning and control *processes* in human organizations” (Anthony, 1965). Anthony’s work also indicates that there should be a direct link between the highest levels of the organization (the strategic levels) with the lowest levels of the organization (Anthony, 1965). We must keep this link in mind when we develop security policy, because the highest levels of the organization must recognize that their decisions can significantly impact the work of their subordinates. This link implies that upper management must work directly with the end user to create effective and unobtrusive security policy.

The KPMG model is a common way for visualizing the whole organization (particularly when this organization is not small), and it is helpful in the discussion of information systems security policy. Anthony’s model illustrates that there can’t be structure in complete absence of process (a common mistake in ISS policy). For a more in-depth look of how the security policy process might actually be implemented & maintained, we suggest the Security System Development Lifecycle model, or SecSDLC.

The SecSDLC methodology is introduced in the recently published book Principles of Information Security (Whitman & Mattord, 2003). The SecSDLC model is based on the standard Software Development Life Cycle (SDLC) model for software development (planning, analysis, design and implementation). The main advantage of the SecSDLC is that it is process-based model with specific steps that can be followed to develop ISS policy.

THE ACADEMIC SECURITY VISIBILITY MODEL (ASVM)

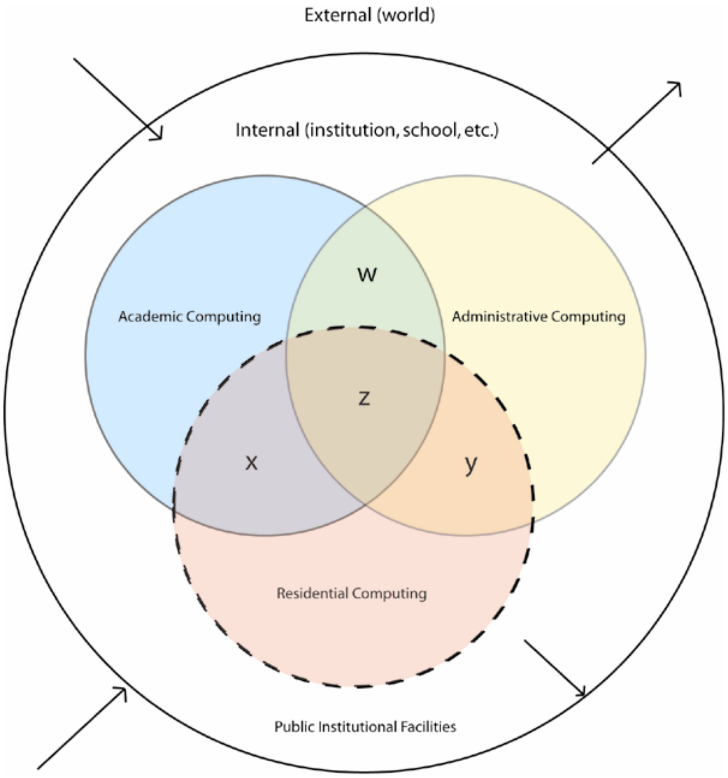


Figure 2. Academic Security Visibility Model

Because of the lack of comprehensive and accessible models for information security policy within the academic environment, we propose the Academic Security Visibility Model, or ASVM. The ASVM can be used effectively in any academic environment irrespective of its size, shape and scope. It is customized for the needs of the academic institution, and can be used in combination with existing frameworks to clarify the security problem domain.

The external entity is everything that is completely outside of the academic institution's control, i.e. the world. The internal entity is everything within direct control of the academic institution. This distinction could be more difficult to make than it seems, because often it is difficult to tell where one organization stops and another begins. However, that is less of a problem because the goal is effective security policy, and effective security policy must specify some degree of separation between what's inside and what's outside the academic institution's control.

Within the internal entity of the ASVM are three major categories or "buckets" of interests, which overlap each other to create a total of seven unique categories requiring different security policies. The three major categories could be referred to as "needs", "users", or "stakeholders" within any given academic institution.

These three major categories are labeled as "academic computing", "administrative computing" and "residential computing". Academic computing represents the needs of students and faculty who wish to use the computer and the network as a learning tool. The stakeholders may require a high degree of freedom and may not wish to be inhibited by security policy. Administrative computing includes all administrative functions that the academic institution needs to undertake, such as working with student enrollment, maintaining student/faculty/staff financial data, grades, etc. This category would require a

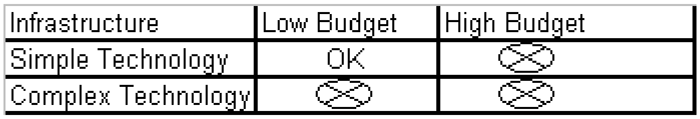
high degree of security because of issues regarding data privacy/protection, and does not necessarily need a high degree of freedom.
Finally, residential computing is an area which is not a part of every academic organization (which is why it is denoted with a dashed line). Residential computing includes both on and off campus use of computing resources by students, faculty and staff, but is specifically such usage which is done from the home. In the case of on-campus students, for example, such residential computing may be from their dormitory. In the case of off-campus students/faculty/staff, such residential computing may include accessing internal school resources from the comfort of their homes or from outside the organization.

It is key to notice the interactions and relationships that occur by overlapping the groups (denoted as w, x, y and z in the diagram). This is a critical aspect of the ASVM model, because it must be assumed that within the organization there are many diverse needs, and some of these needs are not met by the three broad categories of academic, administrative, or residential computing. For example, there may be students who wish to perform academic tasks from their dormitory. This is academic computing, but it is being performed through the residential computing resource. This case is labeled "x" in the ASVM diagram.

One can easily extrapolate what the other letters define, with the exception of the letter z. The label "y" might be a student in a dormitory who wishes to access the administrative computing resource to register for a course. The label "w" might be a professor who needs to report the grades received in an academic project to the administrative computing resource. As already mentioned, the label "x" might be a student doing academic research from their dormitory. The inclusion of these interactions propels these needs to the forefront, making them *visible*.

The label "z" might be confusing; it essentially represents the interactions of all of the internal groups/needs – an essential "common ground". It may be that the label "z" represents a fourth category e.g. the academic institution's Intranet. Also, the academic institution's public computing facilities are depicted in the area surrounding the internal groups. These public computing resources might be public workstations that any of the three other categories (administrative, academic & residential) may have access to. These public resources still require security policy but need a lower level of security than the major computing resources.

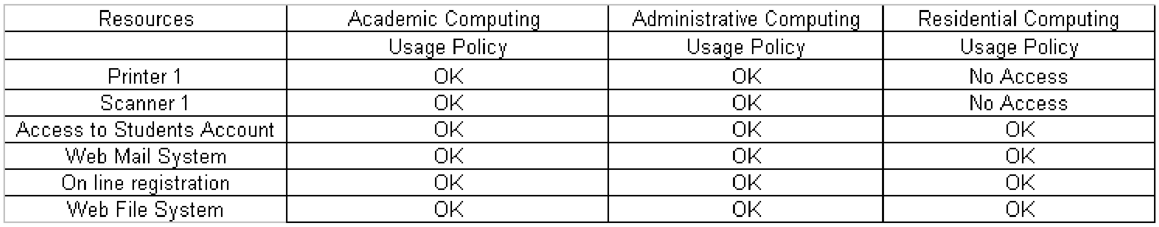
There are also public institutional facilities, which are another vital component of the model. This region, which surrounds the three inner categories, can be treated as a DMZ[1]. This region is a good location for a proxy server. The proxy server can be used for regulating the traffic that travels from one network to other or from outside the network into inside the network. This region is also where wireless network capabilities would be found. Infrastructure is an important component of any policy matter. The infrastructure management matrix shown in Table 1 explains the relationships between different components associated with infrastructure issues in the academic environment.



Infrastructure	Low Budget	High Budget
Simple Technology	OK	⊗
Complex Technology	⊗	⊗

Table 1

The ASVM can be effectively used to understand the complex problem depicted in Table 1, and its long term as well as short-term impacts on the academic environment.

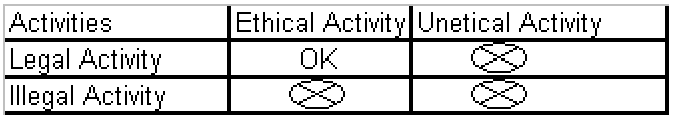


Resources	Academic Computing	Administrative Computing	Residential Computing
	Usage Policy	Usage Policy	Usage Policy
Printer 1	OK	OK	No Access
Scanner 1	OK	OK	No Access
Access to Students Account	OK	OK	OK
Web Mail System	OK	OK	OK
On line registration	OK	OK	OK
Web File System	OK	OK	OK

Table 2

The resource management matrix (Table 2) will provide visibility and will help in formation as well as implementation of security policy for shared resources. Once the appropriate resource management policy is drafted, the next task should be to think about possible activity domains. The activity management matrix (Table 3) will explain the related issues in more detail.

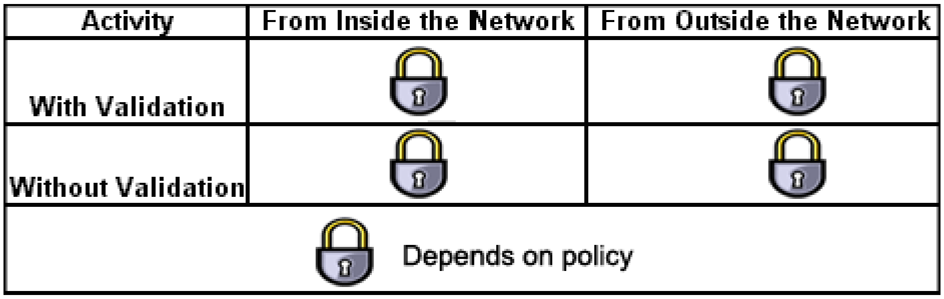
[1] DMZ : demilitarized zone



Activities	Ethical Activity	Unetical Activity
Legal Activity	OK	⊗
Illegal Activity	⊗	⊗

Table 3

The activity management matrix (Table 4), explains a policy based-concept to handle the security and identity related issues in an academic computing environment.



Activity	From Inside the Network	From Outside the Network
With Validation	🔒	🔒
Without Validation	🔒	🔒
🔒 Depends on policy		

Table 4

CONCLUSIONS

The ASVM model can be viewed in many different ways, and has many implications for information security policy within an academic environment. This model presents a very broad network diagram, a map of custom needs and stakeholder groups, a guide for firewall configuration, a starting point for vulnerability analysis, and much more. The power of this model is its flexibility, which revolves around the notion of visibility. The security policy must be sensitive to issues all the way from individual user needs within the organization, to what is actually going on inside the academic network. In other words, these issues must be *visible* to the management to be addressed by a comprehensive security policy.

ACKNOWLEDGEMENTS

We would like to thank Dr. Samir Chatterjee for his guidance in this process, Wayne Smith and Dr. Paul Bishop for sharing their insight into information systems security in the academic environment. Of course, where would be without the love of our families and friends who constantly support our endeavors!

REFERENCES

1. Anthony, R. (1965) *Planning and Control Systems: A Framework for Analysis,* Harvard University, Boston, MA.
2. Bruhn, M. and Petersen, R. (2003) Planning for Improved Security, *Educause Review,* 38, 6, 98-99.
3. Columbia Encyclopedia Online Sixth Edition (2003) Definition of “academic freedom” http://www.bartleby.com/65/ac/academic.html
4. Educause/Internet2 Workshop (2002) Principles to Guide Efforts to Improve Computer and Network Security in Higher Education, http://www.educause.edu/ir/library/word/sec0310.doc
5. Gerber, L. (2001) Inextricably Linked: Shared Governance and Academic Freedom, *Academe,* 87, 3, 22-24.
6. KPMG Information Systems Security Website (2002) http://www.kpmg.com/microsite/informationsecurity/iss4.html
7. Peace, G. (2003) Balancing Free Speech and Censorship: Academia’s Response to the Internet, *Communications of the ACM,* 46, 104-109.
8. Roiter, N. (2001) Security: It's Academic, *Information Security*.
9. Walton, J. (2002) Developing an Enterprise Information Security Policy, *ACM SIGUCCS User Services Conference,* Providence, Rhode Island, USA, pp. 153-156.
10. Whitman, M. and Mattord, H. (2003) *Principles of Information Security,* Thomson Learning.