Technology Policy on Campus

26th Annual Conference on Law and Higher Education
Stetson University College of Law
February 22, 2005

by
Howard W. Bell, Jr.
President
Bell & Trice Enterprises, Inc.

and

Nancy Tribbensee
Associate Vice President for Legal Affairs
Arizona State University

Many professionals in academia have significant experience in developing policy and reviewing risk management strategies. They understand the need to evaluate policies from the perspective of individual constituents, the institution, and the broader community. Academic and student affairs administrators regularly must consider the affect of individual policy decisions on a wide variety of stake-holders. They also regularly evaluate a vast array of programs, from foreign travel to intramurals, to evaluate whether the activity is meeting institutional and individual goals, whether university regulation may have unintended consequences or risks, and the best ways to manage perceived risks to achieve desired results. This policy expertise is a very valuable campus resource.

Campus issues that are highly technologically oriented, however, may not receive the full benefit of this campus-wide expertise. Often the burden of policy-making in these areas falls disproportionately to professionals who work directly with the technology, without meaningful participation from other campus representatives. This is unfortunate, for although the technology community is a valuable and essential resource, they cannot be expected to effectively design or implement institutional policy alone.

Two forces may be at work to limit participation of non-technology types in these policy discussions. First, many on campus may not understand the underlying technical workings of the technology. They may avoid discussions of technology for fear of exposing a potentially embarrassing lack of knowledge.

Second, those in the know (*i.e*., members of the technology community) are so accustomed to making decisions without outside input, that they may forget to invite others to the table as new issues arise. They may also not have sufficient information about institutional priorities or concerns to recognize the need to include others in policy level discussions. This being said, many technology professionals work hard to shift policy considerations to higher administrative levels, and try to include other campus representatives in policy discussions, but are often frustrated by a lack of response to their efforts.

The goal of this paper is to encourage participation in technology policy discussions by campus personnel who do not ordinarily define their roles in terms of technology, but who are important users and beneficiaries of these resources. The discussion will begin with a brief discussion of technology issues generally. It will then focus on an example of one pervasive campus technology, information technology, to provide concrete examples of computing policy issues that are relevant to all campus constituents and suggest ways in which people outside of the technology community can participate in these discussions.

TECHNOLOGY

Many technology policy issues and concerns may be common across multiple types of technology. An essential consideration in individual cases is the role of a particular technology in the overall mission or goals of the institution. The following definitions may be useful to consider when thinking about various types of technology: 1) Utility Technology; 2) Competitive Edge Technology; and 3) Leading Edge Technology.

*Utility Technology***.** A Utility technology is a system that performs a specific task and provides a basic infrastructure platform that individuals and organizations can utilize to perform and create a variety of functions and services. Utility technologies are typically extremely reliable and safe to use, are often provided by a central entity that services the entire user community, and are heavily regulated to ensure uniformity of service and the ability of end users to connect to and use the infrastructure without interfering with or compromising the system. Utility technologies are generally very stable and do not change significantly to meet the specialized needs of the users that are served.

Two technologies that are often thought of as utilities are electricity and water. Within the past decade, the information technology network increasingly has become viewed as a utility technology. As technologies evolve, some technologies that are today considered Competitive Edge or Leading Edge technologies (see the following discussions about these technologies) will likely become Utility technologies.

Competitive Edge Technology. A Competitive Edge technology is a system that, either by itself or in tandem with a specialized program or service, provides an individual or organization with a competitive edge. Competitive Edge technologies are typically extremely reliable and safe to use. While a Competitive Edge technology may be provided by a central entity that serves the entire user community, it can also be provided by a unit within an organization that only serves the needs of that unit. A Competitive Edge technology is often designed to be able to respond to and meet the rapidly evolving needs of the users that it serves.

A Competitive Edge technology may, over time, become sufficiently routine such that it ceases being a Competitive Edge technology and becomes a Utility technology. The information technology network is an example of a technology that was a Competitive Edge technology for some organizations 15 years ago and has gradually become a Utility technology.

Leading Edge Technology. A Leading Edge technology is a system that is designed to push the technical limits of a given technology. Leading Edge technologies are often experimental technologies. As a result, Leading Edge technologies are not always very reliable. They often invite users to test limits, which may cause the technology to be compromised from a security or functionality perspective, and they are typically used by either a small group of users within an organization or a large group of users that enjoy experimenting with technology and are tolerant of technology "glitches."

Over time, a Leading Edge technology may become either a Competitive Edge or Utility technology. When Local Area Networks (LANs) were first used around 20 years ago, they were considered Leading Edge technology.

For purposes of the following discussion, we will focus on information technology policy issues. The reader can generalize from those examples to broader technology issues, keeping the above distinctions in mind.

CAMPUS INFORMATION TECHNOLOGY

Several policy issues in higher education computing and information technology merit broad campus involvement and require the participation of people who rely on these resources, who have knowledge of institutional goals, and who have experience developing institution-wide initiatives. Two examples of significant policy areas that are currently hot topics on campus are: 1) security and privacy, and 2) intellectual property issues. The results of discussions in these areas will have great significance for ongoing campus strategic planning for areas across campus, including areas outside of traditional computing centers. With regard to issues of privacy and security, universal involvement is not only desirable, it is essential to protecting the integrity of valuable campus resources and information.

Security and Privacy

All users of campus computing and communications resources have a role to play in protecting the security of information and systems. The area of security is one that is often left to information technology offices and personnel, until a problem arises or concerns about individual privacy are raised. This is an area which would benefit greatly from active participation by representatives of all campus constituents. All have a responsibility for protecting the integrity of the campus systems and information with which they come in contact. In addition, failures of security or privacy protections may result in institutional liability for negligent security if appropriate practices are not in place across campus.

Good institutional practice with regard to sensitive information and systems can decrease the risk of liability for negligent security. Campus administrators are familiar with claims for negligent security in cases involving dangerous premises or security practices in residence halls or at public events. Similar claims may be on the horizon to address harms that may arise from negligent security for information systems.
Various statutory schema are developing to impose legal requirements for privacy and security relating to specific types of information. Increasing state and federal regulations are imposing responsibility for maintaining privacy of information and some statutes impose requirements that relate directly to the storage of information on computing and communication networks.

While the issues connected with security and privacy cover a continuum of challenges and problems, one can view the issues associated with campus information technology security and privacy, as consisting of two forms of security and privacy threats. One group of security and privacy threats arises from the consequences of privacy and security violations arising from faculty, administrators, staff, and/or students gaining inappropriate access to systems and/or data or using the institution’s systems and/or data in inappropriate ways. The other group of security and privacy threats arise from attacks by worms, viruses, or other system pests on the institution’s systems and data or the outright theft of computer equipment. This paper will refer to the first group of security and privacy threats as System/Data Threats and the second group as System/Data Attacks.

System Data Threats

Campus administrators are very familiar with the privacy requirements of the Family Educational Rights and Privacy Act (FERPA).[1] New questions arise regarding obligations under FERPA, however, when individuals wish to use alternative methods of communication to send or store student information. For example,

- When is it appropriate to use e-mail to send student information?
- What student information can the university provide to a vendor that is offering a student information software package?
- If a courseware package provides information about all students in the class to promote class discussion, how can the institution protect students who do not wish to have directory information released?

The answers to these questions require not only knowledge about the technology but also knowledge of and experience with the requirements of FERPA. They require applying the same analysis used to resolve similar questions that do not involve technology.

Other statutes, such as the Health Insurance Portability and Accountability Act (HIPAA)[2] and the Gramm-Leach-Bliley Act (GLB),[3] include rules for protecting the privacy of health and financial information. In this regard, they are similar to the privacy rules for student information in FERPA. They go beyond the FERPA model, however, in that they also provide rules for maintaining the security of information stored in computer networks or otherwise transmitted electronically. Some states have added statutory

[1] 20 U.S.C. §1232g.

[2] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 42 U.S.C.).

requirements to respond to unintended disclosures of private or sensitive material.[4] One positive consequence of these regulations is that they have forced numerous areas across campus to meet to discuss the best methods for implementing the statutory requirements.

In addition to statutory liability, the potential exists for negligence liability for failing to meet an appropriate standard of care with respect to protecting sensitive data. As more and more statutes such as HIPAA and GLB set security requirements, those statutory requirements may come to influence the expectations of people within the campus community and those outside with whom we relate (such as donors, patrons of campus events, and vendors). Eventually, they may also come to establish a legal standard of care in negligence law for protecting sensitive information not covered by statute.

Everyone across campus, including those with no technology expertise can take some common sense steps to protect the privacy and security information. One important practice is to review the manner in which information is collected, stored, and accessed in the normal course of college or university operations. For example, as paper forms become available on-line, administrators and users should ask whether it is necessary to collect all of the information requested on each form or application. The fewer times the information is collected and stored, the less effort will be required to protect it.

Another area in which traditional risk management techniques can serve well to protect data and systems is the hiring, supervision and termination of employees (including student employees and temporary workers). To the extent that these persons have access to sensitive information or systems, that access should be carefully

[3] 15 U.S.C. § 6801-6809.

monitored. This has always been the case (even before computer networks were used to sort and store information), but the need for technology skills in the workplace has, in some cases, overshadowed traditional common sense employment strategies.

When hiring, supervisors should check references for issues relating to professional integrity, not just to confirm the technology skill set. This is especially important for employees working in areas that regularly work with sensitive data and information or computing resources.

The unit should also provide training for new employees on confidentiality of student records, personnel information, financial information, and other types of sensitive data and information with which they will have contact. Training should also address the requirements for using computing resources, and on protecting system security. Training should also include procedures to prevent employees from providing confidential information to unauthorized individuals, procedures for the proper disposal of documents that contain protected data and information, and procedures for the prompt reporting of suspected problems. It may be appropriate to have some or all employees sign a separate statement acknowledging responsibilities regarding data or access.

Each department responsible for maintaining sensitive data and information, or providing access to sensitive networks or systems, should implement continuing privacy and security training appropriate to the department. As job responsibilities change, through promotion or otherwise, security issues and access privileges should be revisited. Supervisors should limit access to sensitive data, records, systems and equipment to only those employees who have a business reason to know such information. The supervisor should be knowledgeable enough to supervise employees with high level access to

[4] California Civil Code § 1798.82, *et seq.*

systems. No employee should have access to more information than is necessary to perform the job and the person supervising should be confident that the supervisee is not exceeding his or her authority. This can be difficult when a supervisee has greater technology skills than the supervisor.

Finally, if an employee (or student) has had access to sensitive campus systems and data, care must be taken to protect those systems and the information they contain against sabotage before the employee is terminated (or the student is suspended or expelled). Employees should also be advised of potential consequences for misuse of systems or information. System managers and supervisors need to develop protocols for routine termination of employee and student access to data, records, systems (document in employee and student conduct file, if applicable). Before any negative employment action or student conduct sanction is taken against an employee or student with access to sensitive systems or data, the individual's access to critical systems or data should be evaluated. The supervisor should consult with supervisor, university counsel, and the Chief Information Officer (or designee) as necessary to implement appropriate steps to protect systems, data, and other resources. In addition, other employees who may be aligned with the employee or student should be identified and instructed regarding access. Each institution should consider developing an automated process for notice to managers of critical systems (including the Chief Information Officer) of termination, resignation, suspension or expulsion of any employee or student. Some cases may require additional consultation with university counsel (and police, if appropriate) All employees should understand their obligation to report suspicious or unauthorized activity immediately to their supervisor (and police, if appropriate). Many of the same cautions for beginning, maintaining and terminating individual relationships will also apply to cases involving students, volunteers, and vendors.

Another way in which administrators outside of the technology administration can protect security and privacy is to be mindful of the implications of centralization or decentralization of information technology resources. Campuses vary in the extent to which computing resources are centralized under a single administrative office. Many campuses use a hybrid model, which centralizes some information technology functions, but permits others to be managed by various schools, colleges or other offices across campuses. If resources are centralized, administrators outside of that area need to have meaningful input regarding policy issues that affect the campus. For example, if a large courseware software program is purchased, individuals who understand FERPA need to participate in the review of available packages. As decisions about websites are made, offices that appreciate the need to make those websites accessible to users with disabilities need to be involved. Also, before information is downloaded from an institutional database to create a local college or departmental database, the unit should be certain that they are providing the same level of security and access restrictions as was provided at the institutional level.

System/Data Attacks

In September and October 2004, Gartner, Inc., a technology research company, and The Chronicle of Higher Education conducted a survey of 3,000 Chronicle subscribers. Of the 3,000 subscribers surveyed 501 colleges and universities responded. Of the respondents, virtually all of them reported experiencing virus or worm attacks during the past twelve months and 73% of them reported an increase in attacks over the previous year. In addition, while 14% of schools reported unauthorized access to student data, 22% reported the vandalizing of their web sites, and 53% reported denial-of-service attacks.[5] Hence, attacks on system web sites and attacks that cause a denial-of-service occur more frequently than unauthorized access to student data.

A denial-of-service attack, as defined by Carnegie Mellon's CERT® Coordination Center, "is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service."[6] Examples given of denial-of-service attacks are: 1) attempts to "flood" a network, thereby preventing legitimate network traffic; 2) attempts to disrupt connections between two machines, thereby preventing access to a service; 3) attempts to prevent a particular individual from accessing a service; and 4) attempts to disrupt service to a specific system or person. However, as noted by the CERT® Coordination Center, "Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack."[7]

While the above description of a denial-of-service attack may seem somewhat sterile, the impact of such an attack as described by Ken Orgill, the chief information officer at the University of California at San Francisco, which operates three hospitals, presents the life and death consequences that can arise from a denial-of-service attack. As Ken Orgill states in a *Chronicle* article, "when your networks go down, it means that your emergency rooms go down, … Doctors can't get to their medical records, a surgeon

[5] "Colleges Face Rising Costs for Computer Security," *The Chronicle of Higher Education*, Information Technology section, by Andrea L. Foster, December 17, 2004.
[6] CERT® Coordination Center web page located at http://www.cert.org/tech_tips/denial_of_service.html.
[7] CERT® Coordination Center web page located at http://www.cert.org/tech_tips/denial_of_service.html.

who's prepping can't get online resources, and patients can't be admitted to the emergency rooms."[8] Given the truly serious impacts of some of the attacks on the web sites and systems of colleges and universities many institutions are spending increased amounts of money on campus information technology security. As reported from the survey cited earlier, 58% of the respondent schools increased the percentage of their information technology budget that was spent on security. In addition to spending more on information technology security, a number of institutions have or are developing strategic plans and policies to improve system security against attacks.

Many of these plans include a number of hardware and software tactics for protecting the institution's systems to include:

- Antivirus software
- Network scanning devices
- Use of software patches to close gaps in operating systems
- Firewalls
- Spam filters on e-mail servers
- Spyware-control software
- Virtual private networks

Many of these plans also include policies granting the authority to certain individuals on campus to:

- Issue a warning letter telling an individual to stop certain behaviors
- Cutting off Internet access to infected machines that are attacking other campus systems

[8] Colleges Face Rising Costs for Computer Security," *The Chronicle of Higher Education*, Information

- Referring students to institutional disciplinary processes.

An example of the kind of planning efforts underway at various schools is visible in the activities underway at Georgia State University. As reported in the *Chronicle* article cited earlier, Georgia State University created an information-security officer (ISO) position in 2000 whose first order of business was to create a three to five year strategic plan for protecting the University's systems from more than five million hacker attacks per week. To protect the University's system the University has installed security hardware and software that automatically checks students' computers for Windows patches, antivirus programs, firewalls, and worms. In addition, the University's policies gives Tammy Clark, its ISO, the authority to quarantine machines that exhibit problems until security software is installed and the problem is eliminated. The policies also give her the authority to disconnect a students' or a professors' computer from the network if it is causing problems with the university's information systems. This policy allows Ms. Clark to effectively cut off a students' or professors' Internet access. As reported in the *Chronicle* article, the powers conferred by this policy enabled Ms. Clark to cut off a professor's Internet connection "while he was writing a grant application because his computer was infected with a worm that was attacking other campus systems."[9]

Given the impact of the above measures on the culture of a college or university, it is imperative that the development of security plans and policies involve more people than the information technology professionals. Hence, faculty, administrators, students, and the institution's general counsel should all be very much involved in the drafting of these plans and policies. What is more, given the real non-technology impacts of the

Technology section, by Andrea L. Foster, December 17, 2004.

enforcement of these policies on the lives of faculty, students, administrators and staff, like interrupting the drafting of a grant proposal, it is critical that the non-technology impacts of the information technology plans and policies be discussed and taken into account when the plans and policies are being drafted.

However, simply creating plans and policies will have very little affect if: 1) proactive steps are not taken to educate the campus community about the plans and policies; and 2) processes are not developed to encourage voluntary compliance with the plans and policies. For example, if a school provides a service that enables students to download software patches on a regular basis but students do not know about the service, or do not understand the reasons why they need to download the patches provided by the service, or there are no penalties for ignoring the service or rewards for adhering to it, having the service will do very little to make student machines less venerable to attack. For example, according to a *Chronicle* article, the University of Pennsylvania (Penn) has recently instituted a carrot and stick approach to encouraging students to use an optional service that will automatically check each day for software patches and install them on a student's machine.[10] The stick portion of the University of Pennsylvania's approach is to give certain individuals at the university the authority to disconnect from the campus network any student who does not download patches within three days of Penn's releasing them. The carrot portion of the approach is to offer students a chance to win an iPod or a gift certificate to Apple Computer's iTunes music store, which sells songs online, if they take an online quiz about computer security.

[9] "Colleges Face Rising Costs for Computer Security," *The Chronicle of Higher Education*, Information Technology section, by Andrea L. Foster, December 17, 2004.
[10] "Wielding Carrots and Sticks," The Chronicle of Higher Education, Information Technology section, Volume 51, Issue 17, by Andrea L. Foster, December 17, 2004, page A38.

While many of the above measures may seem overly restrictive, the consequences of successful attacks on information technology systems can cripple a school's ability to operate. A successful attack can also compromise a school's data that could have both legal and public relations consequences. In addition, all indications are that the number, innovativeness, and severity of attacks on college and university systems will increase during the next few years. Hence, developing security plans and policies that have broad campus input and support, are enforced vigorously, and are encouraged innovatively are imperative.

The risk of attack are not unique to campuses. In 2003, the United States government issued "The National Strategy to Secure Cyberspace" in response to concerns that terrorists might use computers and related networks to threaten the national infrastructure. (The White House, The National Strategy to Secure Cyberspace (Feb. 2003) available at: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

The National Strategy presents a comprehensive framework for protecting the national information technology infrastructure. It specifically addresses public and private sectors involved in agriculture, food, water, public health, emergency services, defense, information and telecommunications, energy, transportation, banking, finance, chemicals, hazardous materials, and postal and shipping. While outlining a comprehensive strategy for this wide audience, it also specifically calls upon higher educational institutions to improve security for campus systems and to prevent cyber attacks from being launched from or through campus systems. The report also identifies key roles for colleges and universities in developing training programs in which students could learn to protect vulnerable systems from attack.

EDUCAUSE,[11] a leading organization in information technology initiatives for higher education, has initiated numerous efforts to increase awareness of computing security and privacy issues in higher education. EDUCAUSE prepared a response to the national strategy documents in its *Higher Education Contribution to National Strategy to Secure Cyberspace.*[12] EDUCAUSE provides excellent resources related to their efforts to track legislation, influence national policy and communicate the importance of information security to the higher education community.[13] EDUCAUSE also has posted a very helpful resource titled: *Effective Security Practices Guide* on its website.[14] The National Institute of Standards and Technology (NIST) also has published a guidance document titled: *Building an Information Technology Security Awareness and Training Program.*[15]

INTELLECTUAL PROPERTY ISSUES

Other areas of policy making that should include representatives from across campus are those that address intellectual property. Issues here can be broadly divided into the use of intellectual property created by third parties, and the ownership of intellectual property generated on campus or by members of the campus community.

Many campuses have addressed policy considerations regarding who should own the copyright in traditional academic publications and intellectual property generated through the use of significant institutional resources. Often, faculty members who write journal articles or textbooks are permitted to retain the copyright in those works. On the

[11] www.educause.edu.
[12] http://www.educause.edu/LibraryDetailPage/666?ID=NET0027
[13] Id.; See, e.g., Paula T. Kaufman and Peter M. Siegel, *9/11 Legislation and Technology: The Academic Impact*. EDUCAUSE, September/October 2002, p. 86-87. http://www.educause.edu/ir/library/pdf/erm02510.pdf.

other hand, typically the institution will retain intellectual property rights in works created with a significant use of institutional resources.

These expectations require additional policy discussion with regard to course products for distance or asynchronous learning for which faculty provide content, but university personnel provide significant resources. Those who participate will want to receive appropriate credit toward merit and promotion, just as they would have received for publishing journal articles or writing textbooks. These are also important discussions for members of the community who have no direct interest in distance learning or commercialization of courseware because of the implications for distribution of scarce campus resources, the potential for conflict of interest, and the possible creation of incentives that compete with traditional scholarship.

Other issues may arise from the use by campus community of the intellectual property of others, such as file sharing (movie and music downloads). As creators of intellectual property, faculty, staff and students should be encouraged to respect the rights of other creators. At the same time, the campus community needs to assess the claims of music and motion picture producers carefully, in light of the fair use doctrine and other legal protections provided to permit private use of copyrighted materials. Even for uses determined to be non-infringing, however, policy considerations may address the appropriate use of limited campus resources to be sure that systems are available for business and academic use during peak hours.   These policy discussions do not require each participant to understand of the process of file-sharing. They do, however, require broad participation by persons with varied interests and experience from across campus.

[14] http://www.educause.edu/security/guide/.

[15] NIST Special Publication 800-50, available at: http://csrc.nist.gov/publications/nistpubs/.

Strategic Technology Planning

At the start of the 20th century only a few mechanically gifted individuals drove automobiles. In addition, other than being a curiosity to most people and a contraption capable of scaring horses, the impact of the automobile on the physical and cultural structures of society were very minimal. Today, while most people still do not know how to personally perform minimal maintenance on their cars, the strategic issues and concerns arising from their use are debated by millions of average Americans.

During the past 40 years, the impact of information technology on American society in general and higher education in particular has undergone an evolution similar to that of the automobile. Forty years ago the computer was a large mainframe machine taking up an entire climate controlled room. Programming of the machine was done via the submission of punch cards to a punch card reader on site and there was limited institutional data on the machine. In addition, other than the cost of the machine; the utilities, technicians and programmers to support the machine; and the purchasing department's and legal counsel's time reviewing and negotiating the purchase contract, the impact of the computer on the campus culture was minimal. By 1980, twenty-five years ago, much had changed. The once isolated mainframe was now running a number of key administrative systems and storing critical institutional data. Access to the mainframe computers, some of which were referred to as minicomputers, was through a series of dumb terminals scattered across the campus or connected to the main computer via a modem. Around 1980, the very first "personal" computers and local area networks were beginning to appear. At the time of their appearance, the technical experts running many college and university computer centers viewed these two technologies as toys with no significant future as serious computer platforms. However, in fact these two technologies were the start of a revolution in computing that gave individuals freedom from the control of the computer specialists. On a parallel track, society had begun to understand the need for data privacy giving rise to the Family Educational Rights and Privacy Act (FERPA) of 1974 and a number of acts and regulations since then.

By the 1990's decentralized computing across higher education campuses was well entrenched and major debates over the uses and control of technology resources were in full force between deans, provosts, and administrators. By the mid-1990s information technology had made it possible to begin implementing one-stop service for student registration and the creation of distance education courses that could be taken anytime and anywhere by a student. However, unlike the mainframes of the 1960s, with a limited affect on the lives of faculty, students, and most administrators, the one-stop service, distance education courses, and other initiatives made possible by current information technology impact the skills and responsibilities of faculty, students, administrators, and staff. They also affect how students learn and interact with the institution. These initiatives have also had an impact on how data is used and protected, and on the policies and procedures governing how people work and play together on college and university campuses. For all of these reasons, as well as the many issues discussed earlier in this paper, information technology planning must be driven by the larger institutional vision and not be seen as an objective in and of itself. Hence, information technology planning at institutions of higher education should be derived from academic planning at the institution, school, and department levels. Given the tight budgets being faced by higher education institutions, information technology planning must also respond to such issues as leadership of the planning process; sustainable funding; productivity; and faculty, staff, administrator, and student motivation to support the planning outcomes.

These issues of planning leadership; sustainable funding; productivity; and faculty, staff, administrator, and student motivation are central issues for every form of strategic planning. Hence, information technology planning should follow the basic principles of good strategic planning for any endeavor. These planning principles begin with an understanding that planning must be done at three different but interrelated levels to be effective. These three levels are:

- Strategic Planning – The big picture, e.g. where you ultimately want to be at the end of the process. This form of planning should result in agreement on the mission (purpose) and vision (ultimate outcome/goal) of the institutional project that is using information technology, and the core values upon which the endeavor being planned will be achieved (for example, the extent of faculty autonomy vs. the need for swift decisive action by a chief information security officer to limit a faculty member's access to the network to protect the network from outside attack by an infected faculty member's computer.)
- Tactical Planning – How you plan to reach the ultimate goal you want to attain at the end of the process. For example, if my strategic goal is to travel from the Stetson College of Law to Stanford University, some of my tactical choices will be whether I travel by airplane, train, car, or some combination of the three.
- Operational Planning – This is the planning of day-to-day activities. Using the Stetson to Stanford analogy, if I choose to travel by car, how many miles do I

> want to travel each day, where do I want to eat and sleep, and do I need to take the car in for preventive maintenance before I begin the trip.

In addition to the three types of planning there are four planning phases. The four phases are: 1) Strategic Direction Setting; 2) Assessment of Readiness; 3) Implementation; and 4) Evaluation.

Strategic Direction Setting is a process for establishing the vision, mission and guiding principles for engaging in a project. The needs and perceptions of the key stakeholders affected by the project are also identified during this step. Establishing the first draft of a Strategic Direction should come from a small but representative group of the academic and administrative officer ranks, and should include faculty and student representation. An example of a technology with strategic impacts being implemented on a number of campuses across the country is the Enterprise Resource Planning (ERP) system. These systems, which are available from SungardSCT, PeopleSoft SA, and other vendors, make it possible to tie together information from the traditional Financial, Financial Aid, Student, Human Resources, and Advancement/Development software systems. Because these systems are designed to integrate functions, they require a much higher degree of cooperation and collaboration throughout the institution than ever before especially since done properly implementing this software may require re-engineering some or all of the institution’s processes. For example, many of these systems offer a process flow component. This component can help with functions like grant management. Using the grant management example, when a faculty member receives a grant approval notice he/she should enter it into the system. Once the notice of the award is in the system, the appropriate person in the sponsored research office and the grant accountant will automatically be informed by the system that the approval notice has been received. The system can also inform both individuals of tasks they need to accomplish to set up the grant in the system. The system can also track when each of the sponsored research and grant accountant tasks is completed.

Given the power of these tools, it is necessary that the academic leadership articulate the degree of transformation expected in the university's basic mission and the role that modern information technologies should play in that transformation. Because it is not typical within the culture of the academy to consider teaching, research, and service as a process, agreeing to the need to analyze and possibly re-engineer these functions becomes a formidable strategic planning hurdle. This hurdle can only be cleared if there is active support from the university's most senior leadership.

While the establishment of the first draft of a Strategic Direction should arise from a small group of the institution's academic, administrative, faculty, and student leaders, the Assessment of Readiness phase should provide the entire educational community, that will be affected by the process changes arising from the strategic planning process, to comment on their readiness to embrace the direction that has been set. Hence, the Assessment of Readiness phase should involve meetings with the academic and administrative leaders, staff leaders, and faculty and student leaders of the institution to assess their readiness to embrace and implement the strategic direction. While the institution's legal counsel may not be part of the Strategic Direction setting phase, the legal counsel should definitely be included in the Assessment of Readiness exercises.

Implementation involves identifying & executing goals & objectives at the tactical and operational planning levels that support the strategic direction. During this phase Key Performance Indicators (KPIs) are established. KPIs are measures that are tied to and help measure progress towards the goals arising from the strategic, tactical, and operational plans. However, KPIs are NOT the Goals. In addition, it is better to have a handful of significant KPIs than lots of less significant ones that you will tire of reviewing. During this phase there is also a need for significant training of the individuals who will be affected by the system. A major source of difficulty with many system implementations is the inadequate nature of the training that is done. This inadequacy of training often arises not because the training is not offered, but because individuals, especially faculty, claim to be too busy to attend the training or feel that the training sessions are a waste of time. Hence, to be successful, an implementation plan should address ways to overcome the likely resistance of faculty, students, and staff to training. Implementation also involves a form of triaging activities so that those activities that are highly visible and will have a significant impact on the success of the venture are accomplished first while activities that are highly visible, even if they have a limited impact on success, and activities that have a high impact on success even if they are not very visible are accomplished next.

During the Evaluation phase the KPIs established earlier should be used to measure how well the project implementation has worked. This phase is especially important for informing the institution’s decision makers whether the investment in the new, expensive, and potentially disruptive system and institutional re-engineering processes has met, exceeded, or fallen short of expectations. Because of the significant budgetary impact of many of the information technology systems being considered at colleges and universities, being able to evaluate whether the expenditures for information technology have fallen short, met, or exceeded expectations may help justify the ongoing budget expenditures to maintain the system. The evaluations may also suggest changes in how the systems are used.

CONCLUSION

Policy issues that appear to focus on technology issues can have underlying implications for other important policy concerns across campus. Members of the campus community should participate in these discussions, and not leave consideration of important issues only to those with a sophisticated understanding of the relevant technology. Indeed, often important policy implications can be exposed when the details of the technology are stripped away.