Computer Security

Questions to Ask ....
Questions that Need Answers

Louise M. Schudlen
Cornell University
Ithaca, NY

Current technology is putting information and computing into everyone's hands. Even Elementary school students are getting access to the Internet and surfing the net as soon as they develop reading skills. But can or should everything be available to everyone? Of course, the answer is "NO". Can it be secured in the current environment? That depends on your definition of "secured".

This paper looks at the information and services higher education institutions typically deal with and identifies the risks and exposures the current computing environment presents.
Introduction

Higher education is facing more competition, more discriminating customers, and less money. Controlling for every possible risk/exposure is not feasible and not in the best interest of our institutions. What is more important is that the risks and exposures are studied by the technical people and that the costs and benefits of eliminating the risks and exposures are presented to the institution's management and strategic planners for a decision on acceptable risk. Risks and exposures vary depending on the data (staff salary vs. student grades), the business application (writing payroll checks vs. admitting students), the computing environment (mainframe vs. client server), and communications (manual vs. electronic). In some cases, the law defines the security need. In other cases, it is a matter of politics and public relations. Sometimes it is even a matter of competitive advantage in an ever increasing competitive market. Security is not absolute. The best defense is knowing what your institution's risks and exposures are, how to minimize them, and which exposures you are willing to live with.

Computer Security means protecting a computer system against internal failure, human error, attack, and natural catastrophe. The goal is to prevent improper disclosure, modification, or destruction of information or deny service through the use of technological safeguards and managerial procedures. Security and control are a part of the entire computing environment. Security must utilize resources effectively and simultaneously minimize unnecessary interference with business goals, competitive performance, and the user's utility.

Security is a trade-off. The institution's managers and strategic planners must weigh total control and its costs/benefits against an acceptable level of risk. The institution's technical, business, legal and audit professionals can provide information to help management come to an informed decision.

Trends Increasing Risks

The following computing trends are presenting our institutions with incredible opportunities, but at the same time are increasing risks resulting in costly exposures.

The decentralization of hardware, software, data, computing personnel, and even technological decision making is evident in most organizations. With this, most organizations face a multiplicity of platforms and software. There is more to control, more to know, and in some cases it is hard to know what or where it is. There are users creating adhoc reports without controls resulting in duplication of effort and unreliable reports. The increased chance of misapplication of technical control features or lack of controls support by users increases the potential for operating errors and mistakes.

Microcomputing has become commonplace. Originally, microcomputers were used mostly to complement mainframe processing, i.e. a downloaded spreadsheet enabling further data manipulation. Now it is often the platform of choice for institutionally important processing. Unfortunately, the microcomputer environment is still far less secure and standards such as disaster recovery and software change procedures are not as diligently followed as its mainframe predecessor.
Communication and the Internet have revolutionized computing by *opening up access* to the world. Many of our institutions are connected to the Internet. There is more and more reliance upon this information and the communication vehicles computers provide. Many of us base decisions on information we obtained from listservers, bulletin boards, and electronic colleagues (E-mail).

More and more business authorizations and approvals are being conducted entirely over electronic media. Often signatures are only an electronic identifier stored in a data file. *Electronic approvals* are fast, easy and efficient, but to prevent fraud and to stand-up to auditor scrutiny proper controls are imperative.

Many institutions are *outsourcing* some or all of their computing. Many institutions have discontinued in-house systems development in favor of purchased system software. This can give the institution a false sense of security. Even though it is a vendor package your institution is still responsible to ensure that the system has proper controls and is properly implemented within your institution. Most outsource companies and some software package vendors have had their product/service audited. They should be able to provide you with a SAS-70 document citing control weaknesses.

The *technology is changing fast*.. Often with a new technology the security controls come later. In addition to a lack of security mechanisms, there are exposures created when staff are poorly trained and not equipped to properly implement or use the product.

*Students*, our single largest customer, grew-up with this technology and are comfortable with it. They are also very entrepreneurial and actively explore ways to exploit the technology made available to them. It is important that they understand the responsibilities that go along with the use of those resources.

Finally, many institutions are faced with *decreasing funds* and are *downsizing* their operations, particularly their administrative staff. Technology is being looked at to provide the means to accomplish the teaching and research missions of our institutions with less. Segregation of duties will not be possible as a control point, and computers will be relied upon to replace some of the current manual checks and balances. There will also be less IT staff. The industry standard for workstation support is recommended at 1 staff to 50 workstations. At Cornell that number varies from 1:100 to 1:200. Short-cuts are taken. Security administration, and LAN and workstation monitoring suffers. With downsizing and budget cuts comes a decrease in commitment to maintenance, system upgrades, and controls. Doing more with less often results in bypassing controls and security measures to get more work done.

**Security, Controls, and Exposures**

*What needs protecting and why?* Data needs protecting. Some data is protected by law. Our institutions have a responsibility due to 1) State/Federal/Agency Regulations and Requirements and 2) Laws protecting individuals such as FERPA, Privacy, and Labor laws. Compliance with regulations is increasingly important with research moneys becoming more scarce and indirect cost rates being scrutinized. Accounting and Human Resource information needs protection from fraudulent tampering. In other cases, security may be politically desirable.
Software Applications must be well controlled to ensure the institution's computer systems provide reliable information. Hardware, System Software, and data are valuable assets that must be secured and controlled to prevent tampering and guarantee continuing operations.

Finally, there is the misuse of the computing resources themselves. It may be the abuse of the institution's E-mail system or the setting up of a commercial web page on your university's network.

Exposures come in many forms and all can result in loss or harm to the institution. Erroneous recordkeeping, unmaintainable applications, or business interruptions can compromise the integrity of data. With decentralization and the move to smaller, more portable platforms, finding what needs protecting and determining whether there are sufficient controls is becoming more difficult. The key is to identify mission critical operations and the computing they use. Proper controls reduce institutional inefficiencies that would exist if for no other reason than the cost and time that goes into fraud investigations or dealing with a political/public relations problem.

The penalties include:

1) Adverse publicity or loss of reputation,
2) Disruption of service,
3) Downtime: delay: interim operation: recovery,
4) Fraud or embezzlement,
5) Future business or funding losses,
6) Investigations,
7) Litigation,
8) Loss of confidentiality,
9) Loss of goods,
10) Loss of money,
11) Loss of opportunities,
12) Loss of system integrity,
13) Misuse of resources, and
14) Staff disciplinary action.

Where is the Threat Coming From? Children are curious about using the computers...often they come into our university networks using their parents' or a friends' network logon. Hackers break in for the intellectual stimulation or the fun of it. Sometimes they find a logon without a password or one that has an easy password to guess. Enterprising students see the use (abuse) of the computer and network resources as their right simply because they are students at our institutions. Disgruntled employees are a possibility, but usually employee's are just using university resources for their own personal uses. What enables the abuse to occur is sloppy security administration, insufficient computing use and acquisition guidelines or methodology, insufficient or poorly communicated university policies, and insufficient controls over resources. Interestingly enough, hackers are not the number one threat.

<table>
<thead>
<tr>
<th>Information Security Threats</th>
<th>55%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidents and Errors</td>
<td></td>
</tr>
</tbody>
</table>
Employee Dishonesty 15%
Fire, Flood, Earthquakes, Natural Disasters 15%
Employee Revenge 10%
Hackers 5%


Risks and A Sample Risk Analysis

Risk is the probability that a particular threat will exploit a particular vulnerability of the system. A risk analysis is a formal examination of an organization's information resources, controls, and vulnerabilities in both manual and automated systems. A risk assessment identifies and evaluates the types of risks, their probability of occurrence, and their potential adverse impact for an automated information system.

The goal is to manage the risk by identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, and an overall system security review as well as the selection, implementation, testing and evaluation of safeguards. The result should be the institution operating at a level of risk they are comfortable with, an acceptable risk. Management's acceptance of a level of risk must be based on empirical data and supportive technical opinion that the overall risk is understood and that the controls placed on the asset or environment will lower the potential for loss.

Recently Cornell implemented two applications: Employee Essentials (A human resource inquiry client server application) and Faculty Advisor which was made available through the web. Security and control is relative. Cornell does not run encrypted communications, so for years mainframe passwords have been flying unprotected across our network. Consequently, the use of client server and web technologies coupled with Kerberos or Sidecar, a ticket granting application for authorization and authentication (developed at Cornell) though not full-proof is an improvement. What is desirable when any new technology is introduced is a technical identification of the exposures and then for the technical, the auditing, the legal, and the business minds of an institution to identify the risks. Armed with the information, the leaders of the institution must decide whether the risks are worth it.

Risks are the potential for loss, best expressed as the answer to four questions:

* What could happen? (What is the threat?)
* How bad could it be? (What is the consequence?)
* How often might it happen? (What is the frequency?)
* How certain are the answers to the first three questions? (What is the degree of confidence?)

What follows is an excerpt from a risk analysis performed by Cornell Information Technology and Internal Audit for the Faculty Advisor Application recently put into production at Cornell.
Point of Exposures for Faculty Advisor

The key control points for client/server applications at Cornell are:
1) The authentication and authorization servers,
2) The communications media/mechanisms,
3) The client machine,
4) The user security habits, and
5) The application database server.

**Risk 1:** Physical Assault on the equipment. The equipment of concern under these circumstances are the kerberos servers that are providing client authentication, the application servers providing client authorization, and to a lesser degree the routers. These servers are currently in the machine room. If you could get access to them:
   1) You could avoid all authentication and authorization checking and access any client server application of interest.
   2) You could modify data that you should not.
   3) You could damage the security databases cutting off services.

**Control in Place or Compensating Control:** As already stated the servers are in the machine room that is under limited access. Access to the room requires an access card which produces an audit trail of those who have entered the room. One could lock the machines up further, but operators do need access to them if for some reason they need to be rebooted.

**Action Item:** None.

**Risk 2:** Telenet Assault on the server from an idle session. If someone has left the computer session idle an individual could telenet to that machine and use that machine's access to gain access to the servers and control the data acquisition system from the idle machine. This would result with the hacker having full access to whatever the initiated session they teleneted to had.

**Control in Place or Compensating Control:** To do this the hacker would have to know a IP address and query that address during a time of idleness. The probability of this is low.

**Action Item:** None

**Risk 3:** Disaster Recovery and Backups on key security servers. Currently there are no formal action plans or off-site tape backups for the kerberos authentication server.

**Control in Place or Compensating Control:** The fileservers are backed up so the data would be available as long as the tapes are accessible and not damaged.

**Action Item:** Define a disaster recovery plan and make arrangements for off-site backup tape storage.
Risk 4: The security servers are on a commonly used net in CIT. This makes them an easy target for sniffing the lines from within the CCC building. With that they could find out the server’s supervisor password and login directly to the security servers.

Control in Place or Compensating Control: Monitor logins to the server. Investigate unusual activity.

Action Item: Put the machine room on a separate net from the rest of CIT.

Risk 5: IP Spoofing.

Control in Place or Compensating Control: None

Action Item: Do IP check.

Risk 6: Passwords passing in clear text gives access to anyone with a sniffer on the net.

Control in Place or Compensating Control: Kerborize application or use Sidecar.

Action Item: Mandate client/server application guidelines to enforce proper use of security mechanisms.

Risk 7: Client infected with a Trojan Horse.

Control in Place or Compensating Control: None

Action Item: User education and security guidelines/awareness. The need to logout and reboot to insure idle machines were not tampered with. Logging out when application not in use.

Summary of Most Possible Concerns

Individuals getting access to information they should not and using that information inappropriately, such as student grades, social security numbers, sensitive personnel information. This could result in public embarrassment for the institution and privacy litigation or failure to comply with FERPA. Our best protection here is to perform and document a yearly survey of practices on other campuses to make sure we follow an "ordinary standard of care" and are not "deemed negligent" in our handling of sensitive information.

The technical group has added many more risks to the list. The analysis broke the application's exposures down by category: risks due to the application, the use of the network, the use of the web server, etc. In addition, a summary of concerns political, legal, audit, public relations specific to that application's information is being developed. This is a work in progress, which I doubt will ever be complete, but has assisted in the
thought process that needs be part of new system endeavors. In addition, it should be noted several of the action items have already been addressed.

**Risk Analysis 2: Network and FileServer Security**

Identification of risks and exposures to the institution need to be done at all levels. From large applications serving the entire campus community to local office applications. Even in the audit office, you have to ask how secure is data on the audit office fileserver. The server is on a Novell network connected to the Cornell backbone with a dial-in capability. It was discussed that the security risks might justify taking the LAN off the backbone and turning off the dial-in modem. The wealth of information that comes to audit via the network from the university systems and the Internet and the ability to work in NYC on documents in Ithaca make going back to that isolated existence inconceivable. We determined though almost all our work is confidential, only the fraud and irregularity documents would present an unacceptable level of risk if they became available. The solution was a policy that all fraud and irregularity documents would be stored on floppies in locked cabinets.

**Determining What Has to Be Secure - Data Security**

The evolution of data processing from mainframes to distributed processing has put the greatest strain on the attempts to control security from a centralized location point. Distributed processing gives users control over their data processing and to a certain extent responsibility for protecting and securing their own data.

Information must be protected if:
- Its disclosure could cause harm to an individual.
- Its disclosure could cause embarrassment or loss to the institution.
- Its alteration could result in financial loss or incorrect management decisions.
- Its destruction could cause an interruption in critical organization functions.

Historically at Cornell, every piece of data was secured by default, unless otherwise specified. This is impractical from an administration point of view, and undesirable. The university works on information. Now Cornell is reevaluating the securing of data. A data administration function has been created, data stewards or custodians have been define, and the question is being asked is there a good reason for securing the data. The data stewards are entrusted to provide proper protection, maintenance, and usage control of the information and maintaining information utility and availability as well as ensuring authenticity and integrity. They are the institutional person most familiar with the use of the data and the legal and political implications for safeguarding it.

Data security requires: 1) classifying the data, 2) determining the types of security control required, 3) accessing the efficacy of existing safeguards, 4) identifying necessary additions and improvements in security measures, 5) determining the availability of resources, 6) determining the level of security coverage needed, and 8) selecting the appropriate security techniques.

**Securing Personal Data**
The right of privacy an individual's right to determine what personal information can be communicated, and to whom. Privacy is not a constitutional right. Privacy rights have largely developed in the twentieth century, as a mixture of state common law, federal and state statutes, and constitutional law. As a general rule, the courts do not like to get involved in workplace privacy issues. Traditionally, employers, have been allowed great leeway to protect their business by almost any means not clearly illegal. Various cases, both state and federal, have upheld the right of employers to search desks, lockers, file cabinets, and E-mail without a search warrant. Though there are legitimate reasons for companies to do such searches, people do not give up all privacy expectations simply by coming to work.

Under the standard of due care, organizations have a duty to provide for information security. The standard of due care relates back to what the reasonable and prudent person would do in similar circumstances. If a reasonable and prudent person would have foreseen the threat and placed a known countermeasure in place regardless of what the current industry practices are, that may be the context in which a system's negligence will be judged. If managers fail to take actions to make their information systems reasonably secure and as a result someone suffers damages when those systems are penetrated, the organization may be sued.

Information security is still largely an unknown entity to most people, including lawyers. The exact duty with respect to confidentiality, integrity, and availability is still evolving in the courts. Consequently, attorneys are a valuable addition to any information security team. Cornell's Information Technologies Division has recently added a lawyer to their staff. There are several benefits to involving attorneys. They may/can determine that the review findings should be protected under the attorney-client privilege act. They can assist in the interpretations of copyright laws or licensing agreement. And corrective actions recommended by a review team may require legal direction. As a member of an information security team they can assist in the identification of foreseeable threats and countermeasures for those threats, identify standards of due care and the organizational duties to users (including those required by statue), and identify countermeasures for threats, according to what a reasonable and prudent person in similar circumstances would implement.

**Securing Student Data**

The Family Educational Rights and Privacy Act of 1974 (FERPA) requires educational institutions in very specific ways to ensure the confidentiality of student information. Briefly, it prohibits the posting or disclosure without the student's consent of the following information: 1) student social security number, 2) student identification number, 3) courses elected, 4) grades earned, 5) grade point averages, 6) class rank, 7) date of birth, 8) place of birth, 9) home telephone listing, 10) academic and disciplinary actions, 11) the most recent student educational records from the previous educational agency or institution, 12) financial arrangements between the student and the institution, and 13) any other education record containing personally identifiable information.

**Application and System Integration Controls**
Business Applications must be secure to insure only authorized proper transactions occur. The new technologies such as local area networks (LANs), client/servers, and distributed computer environments increase the complexity and level of challenge for controlling the computing environment.

Three level of controls are required: 1) General Business, 2) Application, and 3) Project. General Business Controls include development team qualifications, business reasons for the integration, business resumption, change controls, network controls, and access controls. Application Controls include input edit controls, communication controls, documentation controls, user controls, acceptance testing controls, processing controls, and output controls. Project controls include budgets, schedules, performance measures, and project management.

Policies and Guidelines

Computing is a fluid entity but without a container it just flows uncontrolled, unusable. Policies and Guidelines are the structure that contains it. Policies communicate what is acceptable. Guidelines are examples how a policy might be applied to a specific situation. An outline or checklist of detailed procedures recommended to satisfy a policy. In many cases, policies and guidelines are written after the fact. It is important we anticipate the needs and exposures of the future. In many cases we could look to existing policies for guidance. For example, if I call out-of-town friends from work, I must reimburse the university for the phone call. If I E-mail them instead, I still use the university's resource, but are currently under no obligation to reimburse for the personal use.

The availability and the use of computing and network resources is skyrocketing and our staff, faculty, and students need guidance on what are acceptable ways to use these resources. Recently Cornell had two different sets of enterprising students selling Web services using Cornell facilities. It was not clearly communicated to these students that using Cornell's network resources (a non-profit) for commercial endeavors was not acceptable. Policies and guidelines are being written to fill the gap. There is a network administrators group on campus, a maillist containing everyone identified as a departmental LAN administrators, and a LAN administrators manual. In this Cornell uniformly communicates to those responsible for the installation and maintenance of LAN on the Cornell backbone.

There are numerous areas that institutions should create policy to protect themselves, two come to mind immediately, E-mail and unauthorized microcomputer software. E-mail policy should clearly state 1) whether any messages of a personal nature are permitted on the university's E-mail system, 2) whether messages sent on the E-mail system are subject to examination, at any time, by management, 3) what actions will be taken if E-mail is improperly used.

Unauthorized microcomputer software policy should clearly informed employees of the company's position with respect to the practice of copying software. Every year, numerous software copyright infringement suits are filed. In 1991, the Software Publishers Association filed about two lawsuits a week around the country, seeking damages of $100,000 per violation plus attorney fees. (The National Law Journal (Dec 9,
Software copyright and licensing violations put an entire organization at risk of copyright violation litigation, adverse publicity, ethics degradation, unreliable software, loss of software support, and virus contamination.

Security Awareness

Most security breaches are caused by employees acting in ways that undermine security controls. Usually such action is not deliberate. With the widespread use of microcomputers, many security controls are manageable only by the employees themselves. A security awareness program should cover: 1) What should be protected. 2) What employee actions are required. 3) What employees should do if a problem is found. Each employee should know who is responsible for security investigations and should understand the role of internal auditors, the data security administrator, and anyone else involved in investigating a security problem. The controls are everyone's responsibility and concern, not just the computer professionals.

Employees are more likely to follow instruction regarding security precautions when they understand why security is important and controls are needed. The importance of controls should be reinforced by presenting situations they can relate to; users can quickly understand data vulnerabilities if they realize that there is a personal risk involved. For example, most microcomputer users appreciate the impact that the destruction of their hard disks would have on them.

Security Program Topics

Personal conduct
Password management
Physical access controls, Protecting diskettes, and securing equipment
Environmental controls
Information classification, storage, distribution, and disposal
Securing confidential information
Authorization and Authentication
Errors and Information Integrity-prevention, detection, and correction
Backups and Disaster recovery
Legal issues
Portable computers
Copyrights
Viruses

The top efforts on my list are disaster recovery, software piracy, password management, and quality assurance of custom-developed software (even spreadsheet formulas need to be controlled). Only by educating the faculty, staff, and students about the risks and their personal responsibility for preventing misuse of the institutional information and computing assets can you hope to be successful.

Final Topic: Passwords, Authentication, and Authorization

Passwords are problematic. They are too easily monitored, trapped, copied, and replayed over communication lines and on networks. Too often they are copied or written down.
Often passwords are too simple and easily guessed. Frequently inadvertently they are disclosed when initially assigned or handed out. People shared passwords. Passwords can be learned by observing the user keystrokes or easily obtainable by decoy or deception. Hackers will trade passwords like baseball cards. And quite often, passwords are changed too infrequently (and too frequently changed back to the original). And yet passwords remain the foundation for much of our security.

With the increasing use of networks and of outside access to computer resources, the need for security has never been greater. Authentication is the keystone in a sound security program. Authentication is the act of verifying the identity of a station, originator, or individual to determine the right to access specific categories of information. Also a measure designed to protect against fraudulent transmission is by verifying the validity of a transmission, message, station, or originator. Based on knowledge of who the user is, we can control access, authorize the user privileges to perform functions and manipulate data, allow the use of encryption engines, and effectively hold the user accountable for his actions. Dynamic password technology, whether implemented in hardware or software is a secure, reliable way to obtain authentication.

Summary

Security is, above all, about people and a continuing commitment to secure and control the computing environment from people at all levels and in all parts of the organization. It is not cost-effective to implement more security procedures than a given environment requires. Risk analysis can help define realistic security requirements and therefore control the cost of security. A risk assessment methodology will define assets, review threats, identify security requirements, and select protective counter measures not only for the computer professional in the organization, but more importantly for the operational and executive management.

It is important to organize your institution for security by instituting security policies and standards and guidelines. Make sure your policies and procedures protect what you want/are required to protect. You will need baseline security controls, a basic set of controls that meet a minimum set of standards that should be in place in all properly run data centers, LANs, and workstations. It is useless for an organization to develop policies, however sound, if the technology is unable to support those policies. Laws against back robbery and theft would be meaningless if banks left money in the open with no guards, vaults, or alarms to protect it. A commitment to data security unsupported by necessary technological and administrative methods is worthless.

Most importantly your institution must have a commitment to meaningful data security. This can start with a security awareness program which covers what should be protected, what employee actions are required, and what employees should do if a problem is discovered. In all cases, the assignment of specific individual responsibility for information privacy and security and for everyone in the organization to accept personal responsibility and accountability is essential for success.