Negligent Security: The Duty to Protect Computing and Electronic Resources

Nancy E. Tribbensee

In Lewis Carroll’s *Through the Looking Glass*, Alice was puzzled when she noticed that the White Knight had tied a mouse-trap to his horse’s saddle:

“I was wondering what the mouse-trap was for,” said Alice. “It isn’t very likely there would be any mice on the horse’s back.”

“Not very likely, perhaps,” said the Knight, “but if they do come, I don’t choose to have them running all about.” (Carroll, 1960, p. 298)

Colleges and universities rarely have the luxury of the White Knight to be so completely prepared for every risk management contingency. Increasingly, tight budgets force administrators to choose among various options to manage risks and provide appropriate security. Requests for resources to enhance electronic security must compete with a myriad of other legitimate requests, from faculty salaries to the physical security of the campus community. Each decision to spend money on electronic security must be justified by balancing the cost and convenience of the mousetrap, the likelihood of encountering mice, and the damage they might do if allowed to run about.

The following discussion will focus on one of the elements that must be balanced as resources are allocated to electronic security: the risk of legal liability for negligent electronic security. The purpose of discussion is to provide information for those administrators who must defend their requests for these resources, as well as for those

---

1 Deputy General Counsel, Office of General Counsel, Arizona State University, Tempe, Arizona. B.A. Arizona State University, M.A. Arizona State University, J.D. Arizona State University. This article was prepared as a book chapter for the IT Security in Higher Education Monograph, to be published later this year by Jossey-Boss, a publishing unit of John Wiley & Sons, Inc. For additional information about the Monograph, please contact Rodney Peterson at rpetersen@educause.edu.
who must decide which requests to grant. As used in this discussion, “electronic security” includes software and hardware that is purchased or designed to protect electronic records and to respond to unauthorized intrusions. It also includes the periodic review of campus systems and institutional policies. Finally, it includes the resources necessary to provide education and training for those who use campus electronic information systems.

The discussion of legal liability will be limited to the potential for liability under civil negligence law. Federal and state statutes that regulate the use, disclosure and interception of electronic communications and protect the privacy of the records they contain may contain other sanctions (both monetary and criminal) and should be reviewed separately. These statutes will also be indirectly relevant to negligence liability insofar as they create expectations in those using information systems. They may also be deemed by a court of law to create a standard of care to which the entity operating the system will be held for purposes of negligence liability.

Colleges and universities have considerable experience in evaluating the general risks of campus life and their potential for negligence claims. Administrators are generally familiar with claims for physical injuries that can arise from poorly maintained or unsafe premises. In this context, they routinely balance the cost of repairs or additional security against the likelihood of serious harm.

When it comes to electronic and computing resources, various campus constituencies may disagree as to how best to evaluate risks and the costs to address them. Those who understand information systems also understand their vulnerabilities and may be inclined to devote a greater percentage of resources to protect them. Those whose understanding of these systems is limited to their convenience as a
communications tool may never really focus on the risk and consequences of system
damage or failure; they may have been lulled into complacency by the successful
administration of the system in the past. Consequently, they will be less likely to devote
resources to address security risks they perceive to be minimal. Among the costs for each
campus constituency to consider is the potential for institutional liability if the system
fails, is damaged, or is infiltrated by unauthorized users.

Colleges and universities are responsible for maintaining their physical premises in
a reasonable manner to avoid foreseeable risks to students, employees and visitors to
campus as well as to institutional property. These institutions recognize that they face
potential liability for negligence if they maintain their physical premises in a manner that
facilitates foreseeable harm, even if a criminal third party causes the harm. For example,
stairwells should be lit so users can see the stairs and holes in grass playing fields should
be filled so athletes and others don’t injure themselves. In addition, offices should be
locked at night to deter theft and many student residence halls restrict access after hours
to protect students from non-residents.

Similarly, institutions may be liable for inadequate electronic security that results
in loss or damage. Clearly, they may be liable for losses they cause directly. They may
also be liable, however, for damage they facilitate through inadequate electronic security.
The administrators who allocate resources and implement policies should be advised of
circumstances that can contribute to potential liability both directly and indirectly.

Electronic information and communication systems may be used inadvertently in a
manner that compromises system security or damages or destroys information. External
forces of nature may damage systems or electronically stored records. Stored records may
deteriorate over time in such a way that information is lost. Valuable electronic data may become inaccessible over time if devices to read it are not maintained or if the information is not migrated to another more permanent form of storage.

Records stored electronically may be the target of an attack (e.g., hacking or a “terrorist” attack). They may contain evidence of a crime or other wrongdoing (e.g., stalking, theft, or a copyright violation). Information systems may be used to perpetrate a crime or wrongdoing (e.g., harassment or distribution of a worm or virus). These examples support the need for including electronic resources in periodic campus security and liability audits.

Electronic recourses may also be critical in mitigating risk or avoiding liability. They may provide a means to store data that is safer or more accessible than paper records. They may also provide valuable evidence to be used in the investigation of a crime or other wrongdoing.

Many administrators are already familiar with the allegations that last year Princeton admissions officers broke into Yale’s admissions website to check the admission status of applicants who had applied to both Yale and Princeton. Princeton allegedly used information students provided on its application for admission, such as name, birth date and social security number to access the admissions information on the Yale site. In a news report immediately following the incident, Zager (2002) quoted Bruce Schneier, chief technology officer at Counterpane Internet Security. Commenting on the inadequacy of security on the Yale site, he said, “Don’t call this a hack. [Princeton] just typed in the information requested.” The incident has been the subject of
an FBI investigation, and both universities have had to address campus concerns, the press, and the higher education community.

Few would argue against the need for security. But, how much security is enough? In addition to complying with statutes and other regulatory schema, colleges and universities must evaluate the potential for lawsuits alleging that they were negligent in maintaining electronic systems. Just as every physical injury that occurs on campus does not result in institutional liability, not every loss of data will result in a successful negligence claim. More importantly, important values of campus life can be lost if college and university administrators are not careful to balance their review of legal liability with important policy considerations. The following discussion is intended to provide information about negligence law in a context that promotes thoughtful policy decisions that protect academic values in the context of electronic campus resources.

NEGLIGENT SECURITY

Negligence law provides a civil mechanism to determine who should bear the risk of loss for some harm or injury that has occurred. Filing a negligence claim is not the only way for someone to recover for an injury or harm, however. If an institution’s failure to maintain adequate security for electronic resources results in harm to an individual or damage to records, the injured party may file a civil action for breach of contract or for any of a variety of torts, including as invasion of privacy, conversion, defamation, obscenity, harassment, stalking, fraud, identity theft, or negligence. A number of federal and state statutes that regulate electronic communications also provide for criminal sanctions and the reader is referred to Jacobson and Green (2002) for a comprehensive summary of computer crimes.
This section will limit its focus to the degree to which an institution may be liable under the principles of negligence law in relation to its management of electronic resources. As the intent of this discussion is to provide guidance to administrators, it will review general legal principles and their implications for policy development.

Before an institution can be held liable for negligence, the complaining party must prove four separate elements. A claim may begin with, “My data has been lost” or “Someone accessed my student information without permission,” but unless the complaining party goes on to establish the other required elements of a negligence claim, the institution will not be liable under negligence law.

Negligence liability requires four elements: duty, breach, damages and causation. To establish duty, the complaining party must prove that the institution had a legally recognized duty. Next it must show that the institution breached that duty. The complaining party also must prove that it suffered some harm or damage. Finally, it must show that it was the institution’s breach of duty that caused the harm or damage.

All four elements are necessary to establish a legal claim for negligence. The issues of damages and causation are very fact specific and will need to analyzed on a case-by-case basis. The questions of duty and breach, however, have particular relevance for administrators deciding on security policies outside of the context of an individual lawsuit, however.

The first issue is duty. A legally recognized duty can arise in various ways. It can arise from a contract or promise. It can be assumed in language found in an institutional policy or mission statement. It can be implied by the standard of care in the industry.
A duty can take many forms. An injured party may allege that the institution has an absolute duty to prevent the harm or loss from occurring (e.g., a duty to protect against all unauthorized access). Courts are very unlikely to impose such an onerous burden, however, on any college or university system. In keeping with general principles of negligence law, they are more likely to find that an institution has a duty to take reasonable steps to prevent a foreseeable loss. For example, a court might say that a university has a duty to institute reasonable security measures to protect electronic records from foreseeable attempts at unauthorized access. The “reasonableness” of the steps taken will be evaluated in light of the value of the data and the potential for harm associated with its loss or unauthorized release (Kenneally, 2002).

Public policy will influence the issue of foreseeability. For example, courts have had multiple opportunities to review claims for negligent security in campus student housing. Student housing is another university resource that is subject to unauthorized access by outsiders. Additionally, some invited guests (authorized users) may behave badly, and even criminally, after they are granted access. The question of foreseeability is evaluated on a case-by-case basis in light of the circumstances of the individual case. In reviewing recent cases of assaults that have occurred in residence halls, different courts have come to very different conclusions on the issue of foreseeability. For example, in Stanton v. University of Maine, the Supreme Court of Maine found:

“That a sexual assault could occur in a dormitory room on a college campus is foreseeable and that fact is evidenced in part by the security measures that the university had implemented.” (2001, p. 1050)
In the same year, the Iowa Supreme Court came to the opposite conclusion in *Murrell v. Mount St. Clare College*:

“A college, or any other kind of landlord … is incapable of foreseeing an acquaintance rape that takes place in the private quarters of a student or tenant, unless a specific student or tenant has a past history of such crimes.” (2001)

By analogy, arguably colleges and university system administrators know that constant attempts are made to access institutional systems without authorization, and that is the motivation for security that is already in place. On the other hand, an individual instance of hacking may be unanticipated.

Some intrusion attempts are inspired by the same motivation used to scale Mount Everest: because it is there. Other attempts are more sinister and intend real harm. A recent example that has received much publicity is the theft of medical and other information about military personnel from TriWest Healthcare Alliance in Phoenix, Arizona. In a news release dated December 31, 2002, the President and CEO of TriWest reported the burglary of computer equipment that contained confidential files of more that 500,000 members of the U.S. military. In the press release, TriWest indicates that it does not have knowledge of any use or misuse of the information but acknowledges the potential for “misuse.” The press release also indicated that additional security measures have been taken.

Many have speculated that accurate information about security breaches may be difficult to collect. Companies and other large institutions may be reluctant to disclose vulnerabilities for fear of frightening consumers. In addition, they may be concerned about providing too much information to other would be intruders.
One institutional response to a loss or claim for damages may be to deny the existence of any duty. In litigation, the defendant may have an incentive to deny the existence of any duty to attempt to have the case dismissed or disposed of through a motion for summary judgment. Although this approach has meaning to litigators, it does not assist administrators in making decisions about security before a loss has occurred. In addition, this reasoning does not help administrators make security decisions immediately after a loss has occurred. For example, well before any claims are filed on behalf of military personnel whose information was stolen, TriWest has committed to “enhance security.” A “no duty” argument would not provide any support for enhanced security. Finally, the “no duty” position is not consistent with the personal philosophy of many college and university administrators. They will be more receptive to the position that they have a reasonable duty and to guidance on a strategy to proceed.

In *The Rights and Responsibilities of the Modern University*, Bickel and Lake advocate a “facilitator university” approach to the analysis of duty in college and university negligence cases (1999). They begin by reviewing recent case law to conclude that courts are holding colleges and universities to the same legal standards as other large institutions. Administrators who believe that higher educational institutions are immune from suit need only contact their institutions counsel or risk manager (Vinik, 2002).

In providing strategies to manage the risks associated with negligence liability, Bickel and Lake describe the facilitator university as follows:

> When we think of a facilitator, we think of a guide who provides as much support, information, interaction, and control as is reasonably necessary and appropriate to the situation. (1999, p. 193)
They recognize that a major form of university facilitation is the provision of a range of services to the campus community. They also recognize that although many of these services resemble services provided in the private sector, they have a unique character in the context of the campus environment (1999, p. 194).

Campus computing resources are an excellent example of such a service. Although similar services are available through off-campus providers, campus computing networks are intended to promote education, research and communication in an environment protected by academic freedom. Extending the facilitation model to computing resources encourages colleges and universities to make all decisions about electronic security in the context of this larger educational purpose. Impressive, state-of-the-art security measures that pose unacceptable limits on academic use will not be appropriate. Insufficient security that threatens the integrity of data or allows unauthorized access by those outside the academic community will also not be acceptable. Decisions should be based on a desire to create an environment conducive to research and learning.

Bickel and Lake initially developed the facilitator university model to address the potential for negligence issues that arise in the context of high-risk student behavior. One feature of the campus computing environment that is analogous to managing student behavior is that both areas challenge the institution to work with individuals who may not recognize that any risk exists and to encourage those individuals to change their behavior. The virtue of the facilitator model is that it operates from an orientation of shared responsibility. In the student arena, the challenge is to help young college students, away from home for the first time, to understand the risks they face from alcohol use. In
campus computing, the challenges include helping busy faculty, students and administrators understand the security needs behind admonitions to change passwords, to turn off unused machines and to avoid opening e-mail attachments from unknown sources.

This model is extremely useful as a basis for campus policy development. First, the population that ultimately will be governed by the policy is generally very well-educated and will respond more readily to this approach than to an autocratic dictate to behave differently. Also, it distributes some very important responsibility to those in the best position to manage it. In addition, by promoting a model of shared responsibility, this approach helps to remove information technology personnel from a policing role with which they may not be comfortable. Ideally, through on-going education and peer pressure, co-workers, colleagues and students will slowly begin to adopt better practices with regard to security. Finally, by educating users on the issues related to security, it promotes reasonable expectations as to the degree of security they can reasonably expect.

One way to implement this shared responsibility approach is to institutionalize the computer use policy. Negligence liability can arise from the use of computing and communication systems across campus, so the policy should not relate only to the information technology office. Many other constituencies should be part of its creation and review. It should be seen as a tool to protect and enhance university assets.

To acknowledge the limits of the earlier analogy to campus housing, computing resources present unique challenges. An unauthorized entry into one residence hall does not facilitate unauthorized entry into halls across the county and around the world. Breaches of security in individual computing systems, however, can create the potential
for unauthorized access into other systems connected to the first. This greatly expands the class of individuals and entities that may be affected by security decisions and practices.

Without lessening the focus on steps that individuals can take to promote electronic security, the institution will be in a better position to manage some system-wide risks than will individual users. Awareness created by the shared responsibility model will, however, make it easier for users to understand why certain (often temporarily inconvenient steps) may need to be taken to address a breach of security.

In evaluating campus approaches to electronic security, administrators should consider consulting with the campus risk manager and the entity that provides liability coverage for the institution. These individuals can provide information about the claims experiences of others they insure and the extent of coverage available for electronic security issues. They may also be excellent sources of information regarding risk management strategies appropriate to the environment. In addition, the Clinton and Bush administrations have worked with the insurance industry to find ways to make cybersecurity insurance more widely available (Krebs, 2002). This is important even for institutions that are self-insured or otherwise already have coverage, because it will increase opportunities for higher education institutions to shift the risk of loss for some electronic security issues to other entities by means of inter-institutional contracts.

POLICY ISSUES TO CONSIDER IN AN ELECTRONIC SECURITY AUDIT

This section will review a selection of policy issues that should be included in an audit of campus electronic security. The focus here will be on policy issues, with the assumption that the campus will also seek guidance on technological solutions and will
have the opportunity to receive much unsolicited advice in that area from vendors promoting a variety of products.

The policy issues raised below should be evaluated and addressed in the context of shared responsibility. Each example demonstrates a role for a centralized information technology function as well as for the individual using the system. In the event of loss or damage resulting from misuse of a university system, the injured party may argue that the university had a general duty to prevent any harm from occurring. With appropriate policies and practices in place, the university may be able to take the position that it had a duty to take reasonable steps to avoid foreseeable harm. It can then show the steps it took to discharge this duty, including its efforts to educate the campus community and to implement meaningful security measures. By educating individual users in appropriate security, some losses may be avoided. In the event a loss occurs, liability may be avoided or eliminated.

Negligence claims involving electronic resources may arise in a variety of circumstances. These include: institutional use of resources, individual use of resources, unauthorized use of institutional resources, and failure to maintain or secure resources. Institutional computer use policies should be reviewed from each of these perspectives. Many of the policy issues discussed below can be addressed by referring to existing institutional policies, such as those relating to access to information, records retention, codes of conduct or conditions of employment. Each of those policies should be reviewed to ensure that they will provide appropriate guidance for issues that arise in a computing or electronic environment.
A critical issue for any system will be that of authorized access, including identification of the individuals or entities authorized to use the system. For each class of authorized user, the institution’s policy should identify the level(s) of access and the conditions for continued access. For all users, information technology support staff should receive clear guidance on steps to be taken to limit access of users upon separation from institution or misuse of system. The policy should provide a mechanism for a supervisor or faculty mentor to access data necessary for employment or research functions. This work or education related access should be distinguished from access for employment investigations or law enforcement purposes. The policy should also specify appropriate response and sanctions for cases of unauthorized access.

Once access issues are resolved, the system administrators need to evaluate issues relating to records created (e.g., logs), records retention, and record retrieval. For each record type, the administrator should identify who creates a record, who maintains it, and the length of time it is retained. In addition, decisions must be made as to the medium in which a record will be stored (and if the medium is electronic, the steps to be taken to maintain equipment to read the storage media). Another issue is the ability of the system to identify the user (or station). Some campus systems, e.g., some libraries, permit anonymous use. A desire for enhanced security here may conflict with freedom of inquiry.

In addition to the obvious campus needs for records and data, records retention issues can have particular implications in the context of a lawsuit. Obviously, records should not be deleted or destroyed once a request for records, subpoena or court order demanding them has been issued. Records may, and should, be destroyed in accordance
with records retention schedules, however. For example, an institution may have unnecessarily retained a copy of a record that will be very damaging to its position in pending litigation. Even if the record could have been destroyed earlier if the institution had followed its records retention schedule, it can’t be destroyed after a subpoena for it has been received. On the other hand, if a record is lost or destroyed earlier than the destruction date provided by the institution’s policy, this may encourage speculation that it contained damaging information and was destroyed intentionally.

Finally, privacy issues are critical in any audit of electronic resources. In addition to the issue of unauthorized users discussed above, data may reside on individual machines after authorized uses and be viewed by later users of the machine. An audit should consider whether it is appropriate to install software to remove information “left behind” by normal use. This is especially significant for machines routinely used by multiple users in a common area such as a library, college computing center or residence hall.

An organizational issue that may contribute to the ability of any campus to manage electronic resources and minimize risk and liability will be the question of whether the systems are centralized (under a single or very limited number of points of control) or whether the systems are distributed across campus. Distributed systems may take many forms, but some of the features of concern for the purpose of assessing risk of harm and liability are the extent to which those system administrators are (or can be) properly trained and supervised.

An increasing number of campus units are permitting students (graduate students and student workers) to play important roles as system administrators and in managing
important, often valuable records and data. At a minimum, each student and employee
given this access or responsibility should receive training on the institution’s rules
governing computing resources and any other laws or policies specific to the records or
data. Often this does not occur, perhaps because the hiring units are themselves
unfamiliar with the relevant rules and policies.

Another area of concern is the level of supervision provided to students and others
who are permitted access to valuable campus records. In some cases student workers and
graduate students are placed in these positions because they are more technologically
sophisticated than those whose responsibility it is to supervise them. Negligence liability
could arise if information is lost or misused by virtue of the bad acts of an inadequately
supervised employee or student.

CONCLUSION

Colleges and universities can facilitate their primary education and research
missions by managing the risks associated with information technology and electronic
security using a model of shared responsibility. Any security audit of electronic resources
should consider the value of information stored on systems, the costs to replace that
information, and the damage or injury that might result if the information were disclosed
to persons not otherwise authorized to access it. In addition, the costs to users of being
without the system or having to rely on alternative systems must be considered. Finally,
recognizing that various campus constituencies may assess risks and costs differently, a
team approach to electronic risk management is recommended. An audit team should
include representatives who are intimately familiar with campus electronic
communication systems as well as representatives who are close to each of the various
users, such as faculty, staff and students. Legal counsel and institutional risk management should also be included for their perspective on legal liability.
REFERENCES


