Chapter 4
Liability for Negligent Security: Implications for Policy and Practice
Nancy E. Tribbensee

Computer and Network Security in Higher Education
Mark Luker and Rodney Petersen, Editors

Copyright 2003 Jossey-Bass Inc.
Published by Jossey-Bass, A Wiley Company. Reprinted by permission of John Wiley & Sons, Inc. For personal use only. Not for distribution.
In Lewis Carroll’s *Through the Looking Glass*, Alice was puzzled when she noticed that the White Knight had tied a mousetrap 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 having a White Knight around that is 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 computer and network 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 IT 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 focuses on one of the issues that must be considered as resources are allocated to cyberspace security: the risk of legal liability for negligent computer and network security. The purpose of this discussion is to provide information for those administrators who must justify their requests for enhanced security, as well as for those who must decide which requests to grant.

The discussion of legal liability in this chapter is limited to a review of the general principles of negligence law and the influence of the concept of legal duty on policy development. Federal and state statutes that regulate the use, disclosure, and interception of electronic communications and that protect the privacy of the records they hold may contain other sanctions (both civil and criminal) and should be reviewed separately. These statutes are also 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 establish a standard of care to which the entity operating the system will be held for purposes of negligence liability. The reader is referred to Salomon, Cassat, and Thibeau (2003) for a more comprehensive summary of federal and state laws regarding privacy and security in the higher education environment.

Taking an Institutional Perspective on Computer and Network Security

Colleges and universities have considerable experience in evaluating the general risks of campus life and their potential for negligence claims. For example, 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 about the methods used to eval-
uate risks or to predict the costs to address foreseeable risks. Those who understand information systems and their vulnerabilities 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 risks and consequences of system damage or failure; they may have been lulled into complacency by the successful administration of the system in the past. Decision makers who perceive security risks to be minimal will be less likely to devote resources to address those risks. 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. They also need to protect institutional property from harm or damage. Administrators recognize that their institutions 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 do not 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 nonresidents.

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

Communication and information systems may be used inadvertently in a manner that compromises system security or damages or
destroys information. External forces of nature (for example, floods, tornadoes, and earthquakes) 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 (for example, hacking or a “terrorist” attack). They may contain evidence of a crime or other wrongdoing (for example, stalking, theft, or a copyright violation). Information systems may be used to perpetrate a crime or wrongdoing (for example, harassment or distribution of a worm or virus). These examples support the need for including technology resources and information systems in periodic campus security and liability reviews.

Networked computer resources 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.

How Much Security Is Enough?

“Hackers Seize More Than 50,000 Social Security Numbers from U. of Texas Database” (Read, 2003) and “Hacker Steals Personal Data on Foreign Students at U. of Kansas” (Arnone, 2003). These recent headlines have caught the attention of campuses across the country and sparked discussions of the need to evaluate the security of campus computing systems. Many administrators were already familiar with the allegations that Princeton admissions officers broke into Yale’s admissions Web site to check the admission status of applicants who had applied to both Yale and Princeton. Princeton allegedly used information that students provided on its appli-
cation for admission, such as name, birth date, and Social Security number to access the admissions information on the Yale site. The incident has been the subject of an FBI investigation, and both universities have had to address campus concerns (Zager, 2003).

In light of these incidents, 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 computer systems and networks. 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 important, essential 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.

Civil Liability

Negligence law provides a 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 civil damages for an injury or harm, however. If an institution’s failure to maintain adequate security of its information systems 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 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. The reader is referred to Jacobson and Green (2002) for a comprehensive summary of computer crimes.
General Principles of Negligence Law

The focus of this section is limited to the degree to which an institution may be liable under the principles of negligence law in relation to its management of computer systems and electronic resources. By focusing on one element of negligence, the existence of a legal duty, the section will provide guidance to administrators regarding implications for policy development.

Before an institution can be held liable for negligence, the complaining party must prove four separate elements. The four elements required for negligence liability are duty, breach, damage, 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 its legal duty that caused the harm or damage. A claim may begin with “My data have been lost,” or “Someone accessed my student information without permission,” but unless the complaining party goes on to establish all of the other required elements of a negligence claim, the institution will not be liable under negligence law.

The third and fourth elements, that is, damages and causation, are very fact-specific, so they are not discussed here. These elements will need to be analyzed on a case-by-case basis when a loss is alleged to have occurred. The questions of legal duty, both its existence and breach, have particular relevance for administrators deciding on security policies outside of the context of an individual lawsuit, however. Because an understanding of duty can inform the development of policy, it is discussed in more detail here.

Legal Duty and Its Relationship to Security Policy Development

A legally recognized duty can arise in various ways. It can arise from a statutory obligation. It can be created by a contract or promise. It can be assumed in language found in an institutional policy or mis-
sion statement. It can be implied from control of facilities or from a special relationship between the parties. 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 all harm or loss from occurring (for example, a proposed duty to protect against all unauthorized access). Courts are very unlikely to impose such an onerous burden on any college or university, however. In keeping with general principles of negligence law, courts will look to the foreseeability of the harm. They are 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 college or 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 their loss or unauthorized release (Kenneally, 2002).

An Analogy to Security in Campus Housing

Cases involving security issues that have arisen in campus housing can provide a useful analogy for understanding broader campus security issues. Courts have had multiple opportunities to review claims of negligent security in campus student housing. Like computing systems, student housing is a campus resource that is subject to unauthorized access by outsiders. In addition, some invited guests (authorized users) may behave badly—even criminally—after they are granted authorized access.

In reviewing recent cases of assaults that have occurred in residence halls, for example, different courts have come to very different conclusions on the issue of foreseeability of an assault. The question of the foreseeability of the harm is evaluated in light of the circumstances of the individual case. In Stanton v. University of Maine (2001), 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, however, 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, p. 4).

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

**Institutional Responses to Security Breaches**

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 late 2002 news release (McIntyre, 2003), the president and CEO of TriWest reported the burglary of computer equipment that contained confidential files of more than 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, Tri-West has committed to “enhancing security.” If it had taken the approach that it did not have any duty to safeguard the information, it would not have a legal basis to support 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 duty to implement reasonable security procedures. They can then develop a strategy to determine what level of security is reasonable and appropriate and can then develop a protocol for responding to intrusions or loss of data.

Facilitator University Model

In The Rights and Responsibilities of the Modern University, Bickel and Lake (1999) advocate a “facilitator university” approach to the analysis of duty in college and university negligence cases. 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 (1999) 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”
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, these services 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 computer and network 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 considered 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 rather than simply avoiding liability.

Bickel and Lake (1999) 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, turn off machines that are not in use, disable unnecessary features, and 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 better 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 remove information technology personnel from a policing role with which they may not be comfortable. Ideally, through ongoing education and peer pressure, coworkers, colleagues, and students will slowly begin to adopt better practices with regard to security. Finally, by educating users on the issues related to security, reasonable expectations are promoted as to the degree of security they can reasonably expect.

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 country 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 computer and network security, the institution will be in a better position to manage some systemwide 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.

**Risk Management and Insurance**

In evaluating campus approaches to computer and network security, administrators should consider consulting with the campus risk manager and the entity that provides liability coverage for the
institutions. These individuals can provide information about the claims experiences of others they insure and the extent of coverage available for information security issues. They may also be excellent sources of information regarding risk management strategies appropriate to the environment.

The Clinton and Bush administrations have worked with the insurance industry to find ways to make cybersecurity insurance more widely available (Krebs, 2003). This is important even for institutions that are self-insured or otherwise already have coverage. As cybersecurity insurance becomes more available and affordable, parties will have an increased incentive to lower costs by implementing security and managing risks. In addition, higher education institutions will have increased opportunities to shift the risk of loss for some security issues to other entities by means of interinstitutional contracts.

Conclusion

Colleges and universities can facilitate their primary education and research missions by managing the risks associated with information technology and cyberspace security by using a model of shared responsibility. Any security review of technology and information 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 information security risk management is recommended. The team should include representatives who are intimately familiar with campus communication and information 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 personnel should also be included for their perspective on legal liability.

References


