URMIA Journal

2007–08

UNIVERSITY
RISK MANAGEMENT
AND INSURANCE
ASSOCIATION

The mountains they are silent folk

They stand afar—alone,

And the clouds that kiss their brows at night

Hear neither sigh nor groan.

Each bears him in his ordered place

As soldiers do, and bold and high

They fold their forests round their feet

And bolster up the sky.

—Hamlin Garland (1860–1940), "The Mountains are a Lonely Folk"

Front cover: Rocky Mountains, Colorado
Denver: host city for the 2007 URMIA Conference.

URMIA Journal

2007–08

University Risk Management and Insurance Association

Downtown Denver, Colorado

Photo credit: Denver Metro Convention & Visitors Bureau

National Office
P.O. Box 1027
Bloomington, Indiana 47402
Tel. (812) 855-6683 FAX (812) 856-3149
E-mail: urmia@urmia.org
Web: www.urmia.org

A Professional Non-Profit Forum for the Exchange of Information, Concepts, Practices and Developments Between Higher Education Risk Managers

The food of hope
Is meditated action; robbed of this
Her sole support, she languishes and dies.
We perish also; for we live by hope
And by desire; we see by the glad light
And breathe the sweet air of futurity;
And so we live, or else we have no life.

—William Wordsworth (1770–1850)
"Discourse of the Wanderer, and an Evening Visit to the Lake"

From the President

Welcome to the University Risk Management and Insurance Association's annual journal publication for 2007–08. The journal has a rich history of showcasing topics of interest from the profession of risk management in higher education. While the topics vary in nature, they will explore some of the more relevant risks and hazards of our unique risk environment while providing insight into best practices for managing these risks. In addition, we hope that these articles provoke further discussion and awareness within your institution or entity, supporting your efforts to inform your colleagues who may benefit from the experiences and knowledge highlighted within.

The topics vary from coping with student psychological problems in the aftermath of the Virginia Tech tragedy; to maintaining awareness of national security threats; to preventing computer security breaches that result in identity theft. We know that we have only tapped into a small portion of the broad scope of responsibilities and potential risks within higher education risk management. Yet we trust you will find these articles an informative and valuable resource for your program.

I would like to thank the authors who took the initiative and effort to research and write these articles, the volunteer and committee members who assisted, and the national office staff for their countless hours of hard work and effort in editing and publishing this year's journal for our members. We hope you will enjoy reading it.

Ellen Shew Holland, ARM
President, URMIA (2008)

Contributors

URMIA thanks each of the financial contributors who supported the publication of the 2007–08 edition of the URMIA Journal:

Arthur J. Gallagher

Higher Education Practice Group
The Gallagher Centre
Two Pierce Place
Itasca, Illinois 60143-3141

Gallagher's Higher Education Practice Group specializes in serving the risk management and insurance needs of institutions of higher learning. The education community has long been a core competency of our company, and today represents a significant portion of our business. For assistance in assessing and protecting your institution, please contact your Gallagher Higher Education Practice representative or our Executive Directors, Leta Finch at 802-861-6804 and John Watson at 818-539-1445.

Marsh, Inc.

Global Education Practice
One State Street, 19th Floor
Hartford, CT 06103

For over 38 years, Marsh has been honored to serve the higher education community. Our legacy stems from a company-wide commitment to higher education as a core part of our operation. We have created tailored insurance products and risk management solutions to protect your institution. For assistance please contact your Marsh higher education professional or our Global Practice Leader, Jean Demchak at 860-723-5635 or jean.demchak@marsh.com.

John L. Wortham & Son, L.P.

2727 Allen Parkway, Suite 2000
Houston, TX 77019

As the largest privately held insurance partnership in the U.S., John L. Wortham & Son L.P. places our clients' interests first. This approach includes a higher education practice where we create productive, consultative relationships by crafting innovative solutions for this sector's unique challenges. We invite you to learn about Wortham and our capabilities by visiting our website at www.worthaminsurance.com or contacting Jim McCann, J.D. at 713-346-1220 or jim.mccann@worthaminsurance.com.

Without the assistance of these contributors, this publication could not exist.

Features

7 **Tragedy at Virginia Tech: Student Suicide, School Shootings, and the Campus Mental Health Crisis**
Robert B. Smith and Dana L. Fleming, Nelson, Kinder, Mosseau & Saturley P.C.

21 **The Yin and Yang of an Aging Work Force**
J. Tim Query, Associate Professor of Risk Management and Insurance, New Mexico State University

29 **The Threat Level Is Orange**
Leta C. Finch, Executive Director of Higher Education Practice, Arthur J. Gallagher Risk Management Services, Inc.

41 **Mold in the Environment: The Difficulty of Assessing the Risk**
George H. Bender, Manager of Environmental Health and Safety, Duquesne University

49 **Assessing RMIS Needs for Colleges and Universities**
David A. Tweedy, CMC, Practice Leader for Risk Information Consulting Practice, Albert Risk Management Consultants, Inc.

61 **In Case of Emergency: Selecting a Qualified Air Ambulance Provider**
Denise Treadwell, CRNP, MSN, CEN, CFRN, CMTE, Executive Vice President, AirMed International

69 **The Mixed Motive Instruction in Employment Discrimination Cases: What Employers Need to Know**
David Sherwyn, J.D., Steven Carvell, Ph.D., Joseph Baumgarten, J.D.

83 **Risk Manager as a Grievance Petitioner? Manage Lobbying Risks or Lose**
Pamela J. Rypkema, Risk Manager, Gallaudet University

97 **Identity Theft and Data Loss on Campus—Minimizing and Addressing Risk**
James A. Keller, Esq., and Melissa Hill, Esq., Saul Ewing LLP

Tragedy is a tool for the living to gain wisdom,

not a guide by which to live.

—Robert F. Kennedy (1925–1968), U.S. Attorney General

Tragedy at Virginia Tech
Student Suicide, School Shootings, and the Campus Mental Health Crisis

Robert B. Smith and Dana L. Fleming, Nelson, Kinder, Mosseau & Saturley P.C.

Abstract: The Virginia Tech shootings and other acts of school violence are causing lawmakers, school administrators, and the public at large to reevaluate how educational institutions deal with the mental health problems of students. This article explores the historical context of student violence and examines the events leading up to and surrounding the massacre at Virginia Tech. It further reviews the aftermath of the nation's deadliest school shooting, and the ensuing dialogue about what can be done to prevent future tragedies.

On April 16, 2007, every college and university in the country was asking itself the same questions: *What now? What next? Could we be the next Virginia Tech? Is the next shooter sitting in our English class, turning in page after page of violent malcontent and bloodlust poetry? Does someone on campus have information on a threatening individual that they are afraid or unwilling to share? How do we prevent something like this from happening on our campus? How do we prepare for the unthinkable?*[1] *What is the appropriate response?*

The short answer to these questions might be to turn your school into a minimum-security prison, complete with airport security screening procedures outside every dorm, classroom, and quad. Arm your campus police. Create a SWAT team. Install 24-hour video surveillance, loudspeakers, and sirens to alert students and faculty that the quiet kid from ECON101 has just gone and snapped. Conduct lock-down drills and "practice" for the next massacre.

For those of us who are old enough to remember crouching beneath our desks for protection from a nuclear attack, the utility of such emergency drills may escape us—perhaps rightfully so. In the wake of Virginia Tech, however, colleges and universities are being forced to reexamine the way they deal with students with mental illness and related on-campus emergencies. The complex legal and societal problems associated with mental illness have been laid at the doorstep of colleges and universities for years, but now schools are under more scrutiny than ever before. Not surprisingly, the response has run the gamut from the implementation of new, high-tech emergency notification systems to the augmentation of existing counseling services and other mental health resources.

The real learning opportunity presented by Virginia Tech is not in the latest security measure or mental health screening system.

While these measures may be entirely appropriate for some schools to undertake, they are, by and large, reactionary. The real learning opportunity presented by Virginia Tech is not in the latest security measure or mental health screening system—it is the start of a national dialogue about the legal limitations schools face when dealing with mentally ill students. The shootings at Virginia Tech are a sad but appropriate starting point for this conversation, in which every higher education stakeholder should participate.

Mental Health Crisis on Campus

According to the 2006 National Survey of Counseling Directors, an annual survey conducted since 1981, colleges and universities are seeing an overall increase in deeply troubled students. Ninety-two percent of the counseling directors surveyed believe that the number of students with severe problems has increased in recent years,[2] and 91.6 percent report a growing concern with the number of students with "severe psychological problems."[3]

Another steep increase highlighted by the survey is the percentage of counseling center clients referred for psychiatric evaluation. Counselors estimate that 16.4 percent of their clients are referred for evaluation, an increase from

just 12 percent in 2004.[4] An even more striking increase is the percentage of students on psychiatric medication, up from just nine percent in 1994 to 25 percent in 2006.[5] The survey concludes that this increase may be due in part to counselors' hyper-vigilance and an increased level of concern on campus about liability risks regarding student suicides.[6] But those explanations do not account for all of it; counselors say that more students are already on medication upon entering school.[7]

When asked about other concerns, such as an increase in the number of self-injury reports, the need for better referral resources for students requiring long-term care, and the increased demand for crisis counseling, directors reported heightened concern in every category.[8] They also noted an increase from 2004 in the number of students with eating disorders, an increase in the number of sexual assault cases, and more reports of previous sexual abuse.[9]

The survey is not all bad news for colleges and universities, however. Among participating schools, the number of suicides per 100,000 students is 3.8, which is still far lower than the 15-per-100,000 rate among same-age individuals who are not in college.[10] If these numbers remain consistent, even as the number of students with severe psychological problems increases, one could infer that college and university counseling services are working.

Despite the availability of statistics and hard data like this, predicting suicide is *not* an exact science. According to Robert Irvin, M.D., medical director of a long-term residential treatment program within the Bipolar and Psychotic Disorders Program at Harvard's McLean Hospital, "Unless they have previously acted violently or threatened violence, there's simply no way to predict whether a person will commit a violent act. . . . The greatest predictor of acts of violence is prior acts of violence. Lacking that, we cannot say who will be violent and who will not. . . . There is no reliable predictor of who[m] or who[m] not to avoid."[11]

Tragedy at Virginia Tech: The Shooting Rampage Begins

On the morning of April 16, 2007, Seung-Hui Cho, a student at Virginia Polytechnic Institute in Blacksburg, Virginia, killed 27 students and five faculty members before committing suicide. The massacre included two rounds of shootings and lasted some three hours. Shots were fired in West Ambler Johnston Hall, a freshman dormitory housing 900 students. Two students, Emily J. Hilscher and Ryan C. Clark, were killed. Then, more than two hours later, the shooting resumed in Norris Hall, where morning classes were already in progress. The ordeal ended when Cho turned the gun on himself as police closed in on the building he had chained shut from the inside.

Cho was known as a "loner" on the large Virginia Tech campus. He ate his meals alone, rarely spoke to his fellow classmates, and signed in to one of his academic classes with a question mark, rather than his real name. After graduating from high school in Chantilly, Virginia, about four hours away from Blacksburg, Cho enrolled with a number of his fellow high school classmates at Virginia Tech. In the spring 2007 semester, Cho was a senior, majoring in English. He was also planning a massacre.

Complaints and Concerns from Cho's Fellow Students

Early in his college career, Cho began to exhibit behavior that suggested his troubled mental state. In 2005 he was accused of stalking two female students. One of the students complained of excessive phone calls. She characterized Cho's behavior as annoying, but not threatening. The other student complained about instant messages she received from Cho and reported him to the police, and again indicated that no threats had been made. Both women declined to press charges and Cho was subsequently referred to the university's disciplinary system.

Shortly after investigating Cho on stalking complaints, campus police received a call from one of Cho's former roommates who reported that Cho might be suicidal. Campus police spoke with Cho at length and urged him to seek counseling. He agreed to accompany campus police to an independent mental health facility in Blacksburg, where he would be evaluated. At the facility, a social worker determined that Cho was a danger to himself and others. Based on the social worker's evaluation, a Virginia special justice declared Cho mentally ill and an imminent danger to himself, and issued a temporary detention order. Cho was then detained at a behavioral health center pending a commitment hearing. After another evaluation, a psychologist concluded that Cho was mentally ill but did not present an imminent danger to himself or others, and therefore did not require involuntary hospitalization.

Based on this second conclusion regarding Cho's mental health, a court magistrate released him, ordering outpatient treatment and additional follow-up. It is not clear whether he received such treatment or was ever contacted for follow-up.

Bizarre Behavior Continues

Students were not the only ones who noticed Cho's strange behavior. A number of his English professors found his behavior disturbing and his writing menacing and angry. Some faculty members even complained to police and university administrators. After the shootings, Cho's former playwriting professor, Edward Falco, said in an e-mail to the class, "Cho's behavior was disturbing to all of us—and the English department tried, with the best of intentions, to both get him help and to make the appropriate authorities aware of his disturbing behavior."[12] In September of 2005, Nikki Giovanni, Cho's poetry professor, found his actions and writing so "weird" and "intimidating" that she asked that he be removed from her class.[13] Some female students refused to attend the poetry class with him because they claimed he was discretely taking pictures of their legs and knees from underneath his desk.[14] Giovanni complained to then-head of the English department, Lucinda Roy, who alerted student affairs, the dean's office, and campus police, but in the absence of overt threats to harm himself or others, the school believed its options to be limited.[15] Cho was eventually removed from the class and was tutored individually by the department head. During the hour-long tutoring sessions, Cho rarely spoke and exhibited a palpable anger. Students who had other classes with him claim that his writing and classroom behavior was so "twisted" that they openly wondered whether he could be a school shooter.[16] One student recalls joking to her friends that Cho was "the kind of guy who might go on a rampage killing."[17] Other students, however, merely described Cho as "quiet" and noted that he "would not respond if someone greeted him."[18]

Virginia Tech has come under fire for its response to Cho's behavior, and critics have wondered aloud whether it was appropriate to allow Cho to remain on campus after students and faculty voiced concerns about his mental condition. Chris Flynn, director of the Cook Counseling Center at Virginia Tech, said that once Cho was released from the independent mental health facility, discrimination laws prevented the school from taking any action against him: "We work under discrimination acts . . . we cannot discriminate against the mentally ill, nor do we want to." When asked why faculty concerns about Cho's violent writing were not addressed, university police chief Wendell Flinchum said "the writings did not express any threatening intentions or allude to criminal activity. No criminal violation had taken place."[19]

Critics have wondered aloud whether it was appropriate to allow Cho to remain on campus.

Some have also questioned Virginia Tech's response to the shootings themselves and the school's decision not to "lock down" the campus after the first round of shots were fired early that morning. In response to media inquiries, university president Charles Steger said officials decided not to evacuate campus after the first shooting because they believed it was an isolated incident, "a domestic fight, perhaps a murder-suicide." No one was prepared for the carnage that followed.

Cho's chilling videotaped manifesto, which he mailed to NBC News in between shootings, haunted the airways for days. Cho's multimedia package to NBC included an 1800-word diatribe, 29 photos, and one video. As investigators tried to make sense of it all, Virginia Tech mourned.

Cho's final words were chilling:

> You had 100 billion chances and ways to have avoided today but you decided to spill my blood. You forced me into a corner and gave me only one option. The decision was yours. Now you have blood on your hands that will never wash off.[20]
>
> You had everything you wanted. Your Mercedes wasn't enough, you brats. Your golden necklaces weren't enough, you snobs. Your trust fund wasn't enough. Your vodka and cognac weren't enough. All your debaucheries weren't enough. Those weren't enough to fulfill your hedonistic needs. You had everything.[21]

Not the First: Long Line of Tragedies Pre-Date Virginia Tech

School Shootings: Columbine High School

While Virginia Tech is the deadliest school shooting in American history, it is certainly not the first.[22] Perhaps the closest parallel is the 1999 school shooting at Columbine High School in which Eric Harris and Dylan Klebold killed 13 people and wounded 24 others. The Columbine shooters wore long, black coats on the day of the shootings and were part of a counterculture group called the "trenchcoat mafia." Members of the trenchcoat mafia were considered part of an "anti-clique" movement at the high school focused on resisting bullying and other forms of hazing.

Like Virginia Tech, the Columbine shootings were meticulously planned to achieve a maximum number of fatalities. Harris and Klebold placed two 20-pound propane bombs inside the school cafeteria just before the start of the lunch period and then waited outside in the school parking lot. The two intended to shoot students as they fled from the building following the blast. Fortunately, the bombs never went off, but determined to carry out their plan, the two boys returned to the west entrance of the school and began shooting.

Harris and Klebold ransacked the school, shooting students in stairwells, hallways, the cafeteria, and a science room, until finally committing suicide in the school library. In the aftermath of the bloodshed, the nation tried to make sense of the tragedy. Task forces examined gun control laws, the psychology of bullying, and school security.

Student Suicide: Shin v. MIT

On April 10, 2000, Elizabeth Shin, a Massachusetts Institute of Technology student, set herself on fire in her dorm room. Nine months later her family filed a wrongful death suit against the school and several of its medical professionals and administrators. A Massachusetts Superior Court judge determined that the school's medical professionals, as well as Shin's housemaster and student life dean, shared a "special relationship" with her and they could have or should have reasonably foreseen that she would try to hurt herself.

> The plaintiffs have provided sufficient evidence that [the counseling and support services dean] and [Elizabeth's housemaster] could reasonably foresee that Elizabeth would hurt herself *without* proper supervision. Accordingly, there was a "special relationship" between the MIT administrators . . . and Elizabeth imposing a duty on [the administrators] to exercise reasonable care to protect Elizabeth from harm.[23]

The parents of Elizabeth Shin claimed that MIT was on notice of their daughter's mental problems as early as 1999, her freshman year, when she was hospitalized after overdosing on Tylenol with codeine. Shin's housemaster notified her parents of the hospitalization after obtaining Shin's consent to do so. Following the overdose, Shin received treatment from MIT psychologists and was in close contact with school administrators. Shin continued to suffer from suicidal thoughts and engaged in self-destructive behavior such as self-cutting. In December of 1999, Shin sent an e-mail to a faculty member, in which she admitted that she was contemplating suicide. The message was forwarded to university administrators and an MIT psychiatrist.

Less than a year later, Shin's housemaster brought her to the university infirmary for cutting herself. After being diagnosed with depression, a possible borderline personality disorder, and suicidal ideation, Shin was discharged.

In the weeks that followed, Shin made numerous visits to Mental Health Services, for both scheduled appointments and as a walk-in patient. Reports of these visits uniformly detail Shin's thoughts of suicide, feelings of worthlessness, and routine self-mutilation. An outside therapist who met with Shin on April 4, 2000, told an MIT doctor that Shin needed more treatment than she was able to provide and recommended that she be admitted to an in-patient treatment facility immediately.[24] On April 8, 2000, Shin threatened to plunge a knife into her chest. MIT campus police escorted her to Mental Health Services, where she spoke by telephone to an on-call psychiatrist. Notwithstanding Shin's history of mental health problems, the psychiatrist determined that he did not need to meet with her in person and that it was safe for Shin to return to her dorm room.

Two days later, Shin set fire to herself. Students who resided in the dormitory could smell smoke and hear moaning but could not enter Shin's room because the door was locked. MIT police gained access to the room only

to find Shin engulfed in flames. She succumbed to her injuries four days later.

The Shin case is notable not only for its jarring facts and tragic outcome, but also because the judge's ruling signals that even non-clinicians may be held liable for failing to prevent student suicides. The Shin case also gained national attention because Shin's parents were not notified about her deteriorating mental condition (a parallel to Seung-Hui Cho's case). Although the judge did not touch upon this in her ruling, the issue of parental notification looms large post-Virginia Tech. Laws intended to protect students' privacy rights may deter schools from notifying parents about their children's mental health problems. Knowing when and whether to notify parents about a suicidal student is one of the toughest questions school administrators and counselors face. MIT's then-president Charles Vest called the balance between students' privacy rights and "the obvious interests of parents in knowing how their sons and daughters are doing" a real quandary—one that colleges and universities are still grappling with.[25]

> By not formulating and enacting an immediate plan to respond to Elizabeth's escalating threats to commit suicide, the plaintiffs have put forth sufficient evidence of a genuine issue of material fact as to whether the MIT administrators were grossly negligent in their treatment of Elizabeth. Accordingly, the MIT administrators' motion for summary judgment as to Count VIII for gross negligence is *denied*.[26]

Laws intended to protect students' privacy rights may deter schools from notifying parents about their children's mental health problems.

Schieszler v. Ferrum College

Michael Frentzel, a freshman at Ferrum College in Virginia, had a fight with his girlfriend on February 20, 2000. Campus police and the resident assistant of the dormitory where Frentzel lived intervened in the altercation. A few days later, Frentzel sent a note to his girlfriend telling her that he planned to hang himself. She showed this note to a resident assistant and campus police, who later found Frentzel in his room with bruises on his head, which he said were self-inflicted. In response to the incident, the dean of student affairs required Frentzel to sign a statement promising not to hurt himself. Frentzel signed the statement, in which he intimated that he would commit suicide. Again, his girlfriend turned notes over to college officials and the resident assistant. On February 23, 2000, school officials went to Frentzel's room to speak with him about the notes and found that he had hanged himself with his belt.[27]

In the wake of his death, Frentzel's guardian brought a wrongful death suit against the college, its officials, and the resident assistant. The United States District Court for the Western District of Virginia ruled that the college officials had a "special relationship" with Frentzel, that they knew or should have known there was an imminent probability that he would hurt himself, and consequently, they had a duty to protect him.[28] The parties ultimately settled out of court for an undisclosed sum.

Wallace v. Broyles

In *Wallace v. Broyles*, the court permitted the parents of a varsity football player to proceed with a lawsuit against employees of the University of Arkansas at Fayetteville based on the theory that school officials actually *caused* him to commit suicide. The student was seriously injured in a football game, and required extensive physical therapy and high dosages of Darvocet, a powerful painkiller with mind-altering side effects. The drug was supplied by the university's athletic department. The student's parents alleged that the painkiller was dispensed by the university without proper registration or adequate warnings about the drug's tendency to increase depressive thoughts and behavior.

The court noted that Darvocet is a major cause of drug-related deaths. Warnings associated with the drug include a directive to advise patients "of additive depressant effects of these combinations with alcohol," and Darvocet-related deaths had occurred "in patients with histories of emotional disturbances, suicidal ideation or attempts, or misuse of tranquilizers, alcohol, or other . . . drugs."[29]

> Given the potentially harmful side effects that could result from the unsupervised taking of Darvocet by the athletes, in general, a fact issue is posed that such harm could reasonably have been expected in the circumstances described here, where, it has been said, these defendants had illegally permitted large orders to be indiscriminately accessible to anyone entering the athletes' training room.[30]

The court found that an issue of fact was raised as to whether Darvocet, illegally dispensed by the university athletic department, contributed to or caused the student's death.[31] Although the matter was eventually settled out of court, the ruling signaled that individual school officials may be held liable not only for failing to prevent a student's suicide, but for actually causing it. While the holding of the case is quite narrow, prescribing or dispensing drugs in an illegal manner seems sufficient to trigger this type of individual liability.[32]

Individual school officials may be held liable not only for failing to prevent a student's suicide, but for actually causing it.

Mahoney v. Allegheny College[33]

Chuck Mahoney was a star athlete and honors student. It was not until the beginning of his freshman year at Allegheny College in Meadville, Pennsylvania, that he began to show signs that he was struggling with depression. Mahoney called his parents and told them that he was feeling depressed. They called their family doctor for antidepressants and drove to Allegheny to visit Mahoney and connect him with a school counselor, Jacquelyn Kondrot. Mahoney did well in school, pledged a fraternity, and went to see the counselor.

At the beginning of his sophomore year, however, Mahoney informed Kondrot that he wanted to take all of his drugs and cut his wrists. She obtained his permission to contact his parents and informed them that he was at high risk for suicide. He was voluntarily hospitalized for five days and signed temporary releases allowing Kondrot to speak with his parents and the dean of students about his care. After his hospitalization Mahoney said he felt better, returned to school, and went on to earn a 3.85 grade-point average.

When he began his junior year, Mahoney signed a statement from the counseling center, which stated that the school would protect his privacy except in certain situations—namely, if he ever presented an immediate threat to himself or others. Later that year Mahoney's ex-girlfriend contacted Kondrot to tell her that she and other friends were worried because Mahoney told them he wished he were dead. Kondrot determined that Mahoney was again at high risk for suicide, but based on advice she received from a psychiatrist consultant who concluded that the situation was not grave enough to break confidentiality, Kondrot did not notify his parents.

Over the next few months, Mahoney repeatedly refused Kondrot's requests to call his parents. She was so worried that she even tried to circumvent the confidentiality laws by calling Mahoney at his parents' house, in the hopes that they would pick up. The weekend before Mahoney's suicide, his fraternity brothers contacted the deans to express growing concern that he would hurt himself or someone else.

Mahoney hanged himself with his dog's leash in the fraternity house where he lived on February 11, 2002. That very day he sent several desperate e-mails to Kondrot, who begged him to get more help. His parents blamed the school, its deans, and counselor for not notifying them about their son's ongoing problems or giving them the opportunity to intervene. Mahoney's parents sued Allegheny College, two of its deans, and the school counselor who was treating Mahoney at the time, claiming they each had a responsibility to prevent his suicide.

Before the trial began, the Court dismissed the Mahoneys' claims against the deans, stating that they had insufficient knowledge of Chuck Mahoney's situation to be held liable, leaving only the school and Kondrot as defendants. The jury deliberated for just three hours and returned an 11-1 verdict, finding the school and counselor were not liable.

The verdict sparked debate among privacy law advocates and those who would see privacy restrictions loosened in favor of parental notification:

The college maintained that Chuck was never an

imminent risk for suicide, so his confidentiality couldn't be breached. He was an adult and insisted the school shouldn't call his parents about his problems, college officials testified. They said violating his privacy would have worsened his situation, and that his parents should have shown more active concern, especially after their son was hospitalized as a suicide risk in his sophomore year. They said Chuck's parents should have gotten their son to sign a waiver sent to all students that would have allowed the college to discuss his situation with the family.[34]

The Government Speaks: Report of the Virginia Tech Review Panel

In August 2007, the Virginia Tech Review Panel presented its report on the April 16, 2007 mass shootings to Governor Timothy Kaine of Virginia.[35] The creation of the Review Panel was announced by Governor Kaine on April 19, just three days after the shootings, and was intended "to perform a review independent of the Commonwealth's own efforts" to respond to the tragedy.[36] The panel was comprised of a number of experts in the education fields of mental health, as well as security, including former Homeland Security Secretary Tom Ridge.

In its report, the Review Panel assessed Cho's long history of mental health problems and the governmental response leading up to and during the April 16 massacre. The report further analyzed the logistics of securing the large rural campus; campus emergency response and communications systems; the effectiveness of the university and state mental health screening systems; and the impact of federal and state privacy laws on the university's response to the warning signs exhibited by Cho. In doing so, it made hundreds of recommendations for both lawmakers and university administrators.

The report outlined numerous findings regarding the improvement of emergency preparedness and response measures, as well as the improvement of campus-wide emergency notification systems. Perhaps its primary concern, however, was the return of current privacy laws: there was the near total lack of information sharing between the schools Cho attended and between the various departments at Virginia Tech. The report's detailed mental health history of Cho demonstrates how each school he attended was forced to identify and respond to Cho's mental health problem without the benefit of knowledge acquired by previous institutions.[37] Each institution, from Cho's elementary school, to his middle school, to high school, to Virginia Tech, spent significant time and resources in attempting to help the troubled student. But each time he moved on, the next school would be forced to start with a blank slate.

For instance, Cho's high school instituted an Individualized Education Plan (IEP), which federal law requires in order to maximize the educational development of children with disabilities. Because of Cho's inaudible speech in class (diagnosed as "selective mutism"), his IEP modified grading for oral presentations and group presentations to reflect his communication difficulties.[38] With these modifications, Cho did quite well and received a 3.52 GPA in an honors program.

When he applied to Virginia Tech, the university saw only his grades and SAT scores. Cho's high school never informed Virginia Tech about his special education history. Virginia Tech thus had no way to know about Cho's long history of treatment for mental health disorders, or that his grades were "propped up" due to the IEP.[39] The report blames the narrow interpretation of student privacy and health privacy laws by school administrators for their reticence to share records of mental or emotional problems. The Review Panel concluded that "information critical to public safety should not stay behind as a person moves from school to school. . . . Maybe there really should be some form of 'permanent record.'"[40]

The report also faults various departments within Virginia Tech for not flagging Cho as a threat to other students. Multiple professors in the English department had significant concerns about Cho, and he was the subject of discussions by the university's Care Team. Resident advisors also shared concerns about Cho with their supervisors. He was investigated by the Virginia Tech police after the reports that he stalked female classmates, and was further evaluated by the Cook Counseling Center at least three times. Despite these numerous contacts with persons designed to identify individuals who could pose a danger to others, the lack of information sharing between the various offices contributed to "a failure to see the big picture."[41]

The report recommended that Congress amend the Federal Educational Rights and Privacy Act (FERPA)

with a "safe harbor" provision protecting persons who share student information in the good faith belief that doing so is necessary for health or safety reasons. The panel also recommended that FERPA should ensure that student treatment records are treated just as any other health records would be under the Health Insurance Portability and Accountability Act (HIPAA), thus allowing the sharing of records for treatment purposes. The report does recognize, however, that sufficient flexibility currently exists in FERPA's "emergency exception clause" that would have permitted Virginia Tech to share critical information about Cho with administrators, professors, law enforcement, and his parents. As the panel recognized, "Privacy laws can block some attempts to share information, but even more often may cause holders of such information to default to the nondisclosure options—even when laws permit the option to disclose."[42] Because of an incorrect and restrictive interpretation of FERPA (the university's attorney told the review panel FERPA did not allow the sharing of information on a student like Cho[43]), Virginia Tech was unable to recognize the serious danger posed by Cho until it was too late.[44]

The lack of information sharing between the various offices contributed to "a failure to see the big picture."

A Re-Examination of the Rules

In response to the shootings at Virginia Tech, lawmakers and university officials are re-examining rules that might have helped to avoid the tragedy. Less than two weeks after the incident, Governor Kaine issued an executive order expanding background checks for gun purchases, and at the federal level a number of bills aimed at strengthening gun laws have been introduced.

As the Review Panel was still investigating, lawmakers and university officials had already begun to scrutinize the privacy and discrimination laws that kept Virginia Tech officials from informing the shooter's parents of his troubled mental state or from expelling him for his disruptive behavior.

FERPA (also known as the Buckley Amendment) was instituted in 1974 and was designed to protect students' privacy rights by barring the release of students' educational records, which may include everything from academic grades and disciplinary records to detailed medical histories. It also established guidelines as to when such information could be released. Many university officials—not just those at Virginia Tech—believe that FERPA ties their hands and prevents them from disclosing vital mental health information about students to parents and other third parties.

Tim Murphy (R-Pa), a lawmaker and child psychologist, has proposed legislation that clarifies when schools may release information about a student's mental health under FERPA. The bill, called the Mental Health Cooperation Act for Families and Schools, would clarify when institutions may release information to parents about a student's mental health under FERPA. The proposed legislation would also allow universities to notify a student's parents if the student is deemed to be at risk of committing suicide, homicide, or physical assault, without fear of violating FERPA.

Murphy says that FERPA's current emergency exception (which allows schools to release information to "protect the health of the student") is too vague to be of much use to schools faced with students in crisis. Consequently, he claims, schools may withhold vital information from parents for fear of litigation or backlash from the Department of Education, which is charged with enforcing the law. The proposed legislation would permit schools to release information to parents whenever a mental health professional has determined that a student is at risk of committing suicide, homicide, or physical assault.

HIPAA also bars the release of health records to parents in the absence of a signed waiver by the student. While Murphy's current proposal does not specifically include HIPAA, this law has come under the same scrutiny that FERPA now faces and will likely be re-examined by Congress in order to eliminate any barriers to emergency disclosures.

Another area of concern for universities post-Virginia Tech is the Americans with Disabilities Act of 1990 (ADA). The ADA raises a number of concerns relating to the screening, involuntary withdrawal, and readmission

of students with mental illness to campus. Schools should note, however, that while the law prohibits discrimination against persons with disabilities, including mental illness, the courts have made it clear that schools need not tolerate abhorrent or violent behavior from students, whether the behavior is arguably caused by a covered disability or not.

In the wake of Virginia Tech, some college administrators have posited that disability and privacy laws prevent schools from taking appropriate action against students who exhibit suicidal or violent behavior *until it is too late*. This paints a rather stark picture for colleges and universities that face a growing number of students with mental health issues with each passing year. Thankfully, this is not the whole picture. Disability and privacy laws do not require stalwart inaction in the face of outrageous and uncivilized behavior from students—even students with mental health problems. Though the law, as enforced by the U.S. Department of Education's Office of Civil Rights, may require a school to determine that a student poses an "imminent" threat to himself or others before it can mandate treatment or remove the student from campus, "imminent" does not mean "sometime shortly after the first rounds have been fired."

If colleges and universities believe the law erects too many barriers to the implementation of effective and sensible school policies on this issue, then those schools have a responsibility to lobby for change. The tragedy at Virginia Tech has made the mental health crisis on college campuses part of a heated national debate. This puts the higher education community in a unique and powerful position to demand that legislatures and regulatory agencies ease the current restrictions and confusion surrounding the legal duties owed to students with mental health problems, where such students pose a threat to themselves and others.

The tragedy at Virginia Tech has made the mental health crisis on college campuses part of a heated national debate.

What Now? What Next?

While it is tempting to buy the latest emergency notification system off the shelf, institute more training for counselors and student life staff, and implement a lockdown system for on-campus emergencies, unless these and other efforts to reduce risk are coordinated to meet your school's unique needs, they will not be effective. By failing to undertake a formal legal review of your school's programs and policies as they relate to mental health, student affairs, and campus safety, you may miss opportunities to implement truly thoughtful, systemic changes (where necessary) and risk eliminating *lawful, time-tested* procedures that are already in place.

A formalized risk audit can help identify loopholes and weaknesses in school policy, assessing and reducing risk as well as managing liabilities in a good faith effort to prevent student suicide or school shooting. Such an audit often entails one or more of the following:

- A review of the school's mental health policies, including but not limited to: confidentiality waivers, involuntary withdrawal policies, and re-admittance procedures for students returning from medical leave.
- A review of campus safety and emergency response procedures with attendant assessments of the resources available to schools in the immediate aftermath of a student suicide, shooting, or similar tragedy.
- A review of student conduct codes and disciplinary procedures relating to the removal of students from campus and the scope of acceptable behavior permitted in dormitories, classrooms, and common areas throughout campus. Training of administrators, faculty, and staff on the actions that may be taken with a student in crisis, which comply with existing law.

The audit should be conducted by experienced legal, medical, and educational professionals. The audit committee may include, for example, the school's attorneys, risk managers, deans, counselors, campus security officers, and other officials with the power to change and implement new policy on an as-needed basis. This multi-disciplinary approach to liability assessment ensures that the recommendations of the formalized risk audit are consistent with the school's legal obligations, as well as its unique educational mission.

The audit would allow a school to clarify its policies and reduce risk across many areas of student life at once. Where appropriate, such audits may also encourage the development of more proactive measures to address students' pressing mental health needs. In all cases, the risk audit is designed to reduce liability within the current legal framework of federal and state disability and privacy laws.

While there is no one answer to the questions, "What now? What next?" conducting a comprehensive audit is a good first step. Whether you are a Big Ten school or a small liberal arts college, it is recommended that all institutions conduct a formal legal review of their existing policies with advice from experienced legal professionals. As the list of school shootings and student suicides suggests, no one is immune from these tragedies.

About the Authors

Robert B. Smith leads the College & University Practice Group at Nelson, Kinder, Mosseau & Saturley P.C. in Boston and Manchester, New Hampshire. His 26 years of litigation experience includes fourteen years as Associate General Counsel for Boston University, the nation's fourth largest independent university. While at BU, he won numerous jury trials in state and federal courts involving claims of employment discrimination, disability discrimination, student affairs, academic freedom, police matters, contracts, and tort claims. He has also counseled multiple university departments and senior university management concerning the panoply of legal issues confronting modern higher education. He resides in Walpole, Massachusetts, with his wife, Lynne, and children, Zachary and Avery.

Dana L. Fleming formerly worked for Nelson Kinder Mosseau & Saturley P.C., after graduating from Boston College Law School. Her work has involved advising school administrators, program directors, and risk managers on a variety of different legal issues including trial litigation. While pursuing her law degree, Ms. Fleming also earned a master's in education administration from the Lynch School of Education at Boston College. Before law school, she worked as an education researcher in Cambridge, Massachusetts, and studied domestic education policy at the Woodrow Wilson School of Public and International Affairs at Princeton University.

The authors gratefully acknowledge the contribution of Laurie Bishop, a second-year law student at Northeastern University School of Law, who will join the firm in 2008.

E-mail comments to: rsmith@nkms.com.

Appendix A

School Shootings

- ***August 1, 1966***—Charles Whitman, a student at University of Texas at Austin, killed 14 and was shot and killed by police.
- ***July 12, 1976***—Edward Charles Allaway, a custodian at California State University, Fullerton, killed seven, and was later committed to state mental hospital.
- ***January 29, 1979***—Brenda Ann Spencer, a 16-year-old who lived across the street from Cleveland Elementary School in San Diego, wounded eight children and killed the principal and a custodian, confessed and was jailed.
- ***January 20, 1983***—David Lawler, an eighth grader at Parkway South Junior High School in St. Louis, killed one classmate and wounded another before shooting and killing himself.
- ***January 17, 1989***—Patrick Edward Purdy, a drifter, shot and killed five children at Cleveland Elementary School in Stockton, Calif., before killing himself.
- ***December 6, 1989***—Marc Lepine, 25, killed 14 women at the École Polytechnique de Montréal, Quebec, before killing himself.
- ***November 1, 1991***—Gang Lu, a Chinese physics graduate student at the University of Iowa, killed five and then committed suicide.
- ***August 24, 1992***—Dr. Valery Fabrikant, former associate professor of mechanical engineering, shot and killed four professors at Concordia University in Montreal, Quebec, and remains in jail today.
- ***December 14, 1992***—Wayne Lo, a Taiwanese immigrant and student at Simon's Rock College

of Bard in Great Barrington, Mass., killed a student and a professor, confessed and was jailed.

- ***November 15, 1994***—Jaime Rouse, a 17-year-old student at Richland High School in Lynnville, Tenn., killed a student and teacher and was sentenced to life in prison.
- ***February 2, 1996***—Barry Loukaitis, a 14-year-old, killed three at Frontier Junior High in Moses Lake, Wash., and received two mandatory life terms.
- ***October 1, 1997***—Luke Woodham, a 16-year-old, killed his mother and two classmates at Pearl High School in Pearl, Miss.
- ***December 1, 1997***—Michael Carneal, a 14-year-old, killed three students at Heath High School in West Paducah, Ky., and was sentenced to three concurrent life sentences.
- ***March 24, 1998***—Mitchell Johnson, 13, and Andrew Golden, 11, killed four students and one teacher at Jonesborough School in Craighead County, Ark. Both were released from jail at the age of 21.
- ***May 20 and 21, 1998***—Kipland Kinkel killed both of his parents and two classmates at Thurston High School in Springfield, Oreg.
- ***April 20, 1999***—Eric Harris, 18, and Dylan Klebold, 17, seniors at Columbine High School in Jefferson County, Colo., killed 12 students and one teacher before committing suicide.
- ***April 28, 1999***—A 14-year-old killed a student at W.R. Myers High School in Taber, Alberta, Canada.
- ***May 20, 1999***—Thomas Solomon, Jr. (T.J.), a sophomore at Heritage High School in Conyers, Ga., shot and injured six students and has since attempted suicide on a number of occasions, but has failed.
- ***March 5, 2001***—Charles Andrew Williams, a 15-year-old student at Santana High School in Santee, Calif., killed two students.
- ***January 16, 2002***—Peter Odighizuwa, a Nigerian former student at Appalachian School of Law in Grundy, Va., killed two faculty members and a student and was sentenced to multiple life terms in prison.
- ***April 26, 2002***—Robert Steinhauser, a student expelled from the Johann Gutenberg Gymnasium in Erfurt, Germany, shot and killed 16 people before committing suicide.
- ***October 21, 2002***—Huan Yun "Allen" Xiang, a student, killed two at Monash University in Melbourne, Victoria, Australia.
- ***September 24, 2003***—John Jason McLaughlin, 15, killed two classmates at Ricori High School in Cold Spring, Minn.
- ***February 3, 2004***—Michael Hernandez, an eighth grader at Southwood Middle School in Palmetto Bay, Fla., stabbed and killed his friend in a school bathroom.
- ***March 21, 2005***—Jeffrey Weise, a student at Red Lake High School in Red Lake, Beltrami County, Minn., killed his grandfather and his grandfather's girlfriend before going to school and killing seven more people and committing suicide.
- ***November 8, 2005***—Kenneth Bartley Jr., 15, killed a school administrator and wounded two others at Campbell County High School in Jacksboro, Tenn.
- ***September 13, 2006***—Kimveer Gill killed one and shot himself at Dawson College in Westmount, Quebec.
- ***September 27, 2006***—Duane Roger Morrison, 53, entered Platte Canyon High School in Bailey, Colo., and sexually assaulted a number of female students before killing one and himself.
- ***October 2, 2006***—Charles Carl Roberts, IV, 32, killed five girls and himself at West Nickel Mines School in Lancaster County, Penn.
- ***September 29, 2006***—Eric Hainstock, a freshman at Weston High School in Cazenovia, Wisc., shot and killed the school's principal.
- ***December 12, 2006***—Shane Joseph Halligan, 16, a high school student at Springfield Township High School in Springfield, Penn., brought a gun to school and shot himself in the hallway.
- ***January 3, 2007***—Douglas Chanthabouly, a junior at Henry Foss High School in Tacoma, Wash., shot and killed another student.
- ***April 16, 2007***—Seung-Hui Cho shot and killed 32 people at Virginia Polytechnic Institute in Blacksburg, Va., before killing himself.
- ***May 23, 2007***—Two 17-year-old students at C.W. Jeffries Institute in Toronto, Ontario, killed a 15-year-old student.

- *September 21, 2007*—Two Delaware State freshmen were shot in the early morning after a fight between students on a campus parking lot. Delaware State freshman Loyer D. Bradsen has been charged in the shooting. The victims have survived. The campus was initially locked down, demonstrating the lessons of the Virginia Tech shooting.
- *September 30, 2007*—a University of Memphis football player was shot and killed on campus. The assailant or assailants have not been apprehended.

Endnotes

1 Although many describe the Virginia Tech shootings as unknowable, unthinkable, and unforeseeable, the accompanying chart of school shootings suggests the contrary. See Appendix A.

2 National Survey of Counseling Directors, 2006, Item 18.

3 Ibid. at item 20.

4 Ibid. at 17.

5 Ibid. at 15.

6 Ibid. at 40(i).

7 Ibid. at 16.

8 Ibid. at 26.

9 Ibid.

10 Ibid. at 29.

11 As quoted in Daniel J. DeNoon, "Va. Tech Gunman: Warning Signs? Experts Say Cho's Violent Acts Were Not Predictable," WebMD Medical News, April 18, 2007, http://www.webmd.com/mental-health/news/20070418/va-tech-gunman-warning-signs.

12 See http://www.cnn.com/2007/US/04/18/vatech.professor/index.html.

13 Ibid.

14 See http://www.time.com/time/nation/article/0,8599,1612003,00.html.

15 Ibid.

16 See http://www.cnn.com/2007/US/04/18/cho.profile/index.html.

17 See http://www.msnbc.msn.com/id/18248298/site/newsweek/page/5/.

18 See http://www.msnbc.msn.com/id/18148802/.

19 See http://www.cnn.com/2007/US/04/18/vtech.shooting/index.html.

20 See http://featuresblogs.chicagotribune.com/entertainment_tv/2007/04/what_follows_he.html

21 Ibid.

22 See http://www.nytimes.com/2007/04/16/us/16cnd-shooting.html?ex=1192334400&en=305721272cfa098d&ei=5087&excamp=GGGNvatech

23 Not Reported in N.E.2d, 13 (Mass. Super. 2005) (J. McEvoy).

24 See "Elizabeth Shin Chronology," *The Tech,* Vol. 121, Issue 70, Jan. 30, 2002.

25 "Privacy vs. Protection: How Should a College Tell Parents When a Student's Health or Safety Seems at Risk?," *The Christian Science Monitor,* Feb. 12, 2002.

26 *Shin v. MIT,* 19 Mass L. Rptr 500 (Mass. Super., 2005).

27 *Schieszler v. Ferrum,* 236 F. Supp. 2d 602 (W.D.Va., 2002).

28 Ibid.

29 961 S.W.2d 712, 717 (Ark. 1998).

30 Ibid.

31 Ibid. at 719.

32 Ibid. at 718-19.

33 *Mahoney v. Allegheny College* did not generate a published opinion by the court. Accordingly, the facts set forth herein were taken from published reports, media, and other sources.

34 Elizabeth Bernstein, "After a Suicide, Privacy on Trial," *Wall St. Journal,* Mar. 24, 2007 at A1.

35 Va. Tech Review Panel, Mass Shootings at Virginia Tech April 16, 2007: Report of the Virginia Tech Review Panel (2007) (hereafter Report of the Review Panel), available at http://www.governor.virginia.gov/TempContent/techPanelReport.cfm. The Review Panel's report was the most anticipated and publicized analysis of the tragedy, although both the federal government and Virginia Tech itself had previously released reports. See e.g., Report to the President on Issues Raised by the Virginia Tech Tragedy (June 13, 2007), available at http://www.hhs.gov/vtreport.html; Presidential Internal Review: Working Group Report on the Interface between Virginia Tech Counseling Services, Academic Affairs, Judicial Affairs and Legal Systems (Aug. 17, 2007), available at http://www.vtnews.vt.edu/documents/2007-08-22_internal_communications.pdf.

36 Report of the Review Panel, *supra* note 35, at vii.

37 This mental health history is contained in Chapter 4 of the Report of the Review Panel, *supra* note 35.

38 Ibid. at 38.

39 Ibid.

40 Ibid. at 39.

41 Ibid. at 52.

42 Ibid. at 63.

43 Ibid. at 63.

44 Cho's parents told the panel that they would have pulled him from school and gotten him help if they had known of his increasingly antisocial behavior during 2005. Id. at 49.

The mind sees the world as a thing apart,

And the soul makes the world at one with itself.

A mirror scratched reflects no image—

And this is the silence of wisdom.

—Edgar Lee Masters (1868–1950)

"Ernest Hyde," *Spoon River Anthology*

Forty is the old age of youth; fifty the youth of old age.

—Victor Hugo (1802–1885), French writer

The Yin and Yang of an Aging Work Force

J. Tim Query, Associate Professor of Risk Management and Insurance, New Mexico State University

Abstract: Yin and Yang are representations of complementary opposites rather than absolutes, which could describe the situation surrounding an aging work force. This article explores the challenges and opportunities organizations must consider in hiring and retaining older workers.

Introduction

Like many other organizations, colleges and universities are faced with a challenging demographic issue involving the work force. In 2014, some 78 million Baby Boomers will fall between the ages of 50 and 68. About 31 percent of those 55 and older were in the workforce in 1984. That number climbed to 36 percent in 2004, and the figure will jump to 41 percent in 2014, according to the Labor Department's Bureau of Labor Statistics. For Baby Boomers, born between 1946–1964, it is becoming normal for 50-year-olds to go back to school and for 70-year-olds to reinvent themselves through new careers (Mooney 1997). The challenge of "Gray2K" (as coined by some) is one that all institutions of higher learning will need to address sooner or later. A variety of research around the world shows that outdated HR views of older workers continue to exist. The bias against workers over the age of 50 includes claims that older workers are expensive to sustain, adapt poorly to change, find it difficult to interconnect with younger workers, and provide a substandard return on investment for training purposes. However, progressive thinking is beginning to recognize the unique potential of experienced older workers. According to Louise Rolland, a professor studying aging and work at Swinburne University in Australia, "Planning and verbal abilities actually peak in people's 50s and 60s." Workforce researcher Juhani Ilmarinen of the Finnish Institute of Occupational Health believes that, "With age, social skills get better—getting on with people, understanding people, working together and accepting differences." Ken Dychtwald, author of a World Future Society study in 2005, predicts the Boomers will postpone old age by disposing of the current "linear life" culture in which people move lockstep through life, first through education, next through jobs, and finally through leisure and retirement. Instead, according to Dychtwald, a new "cyclic life" Baby Boomer culture is taking shape. Education, work, and leisure will be intermingled repeatedly throughout the life span. This phenomenon coincides with the increasingly rapid obsolescence of knowledge and the resultant growing importance of lifelong learning (Gordon 2007).

Progressive thinking is beginning to recognize the unique potential of experienced older workers.

This paper examines the issues most germane to the aging work force situation—potential skilled labor shortages; health and safety concerns for the mature worker; job restructuring to fit the changing physiology of older workers and meet their need for self-actualization; aging faculty members; and regulatory influences on the retirement decision. Some of these areas are pertinent for university risk managers, while others fall under the authority of other disciplines. However, an awareness of all these issues should provide a broad foundation for the aging work force dilemma.

The Labor Shortage

Not only will the future employee base have a higher average age, but projections of a labor shortfall in just a few years have ranged from two to 10 million people. Based on sheer numbers alone, finding skilled Baby Boomers to fill ever-widening skill gaps over the next 15 years will require a revamping of human capital strategy. While the shortage will be mitigated to some degree by immigration, the significant percentage of specialized personnel that make up the university work force still remains an area of concern. It is particularly true for people with master's degrees and doctorates in fields such

as physics, chemistry, and engineering. More restrictive immigration rules instituted after the terrorist attacks of September 11, along with competing opportunities in other places, may be lessening the attraction of a U.S. education for top students around the globe (Bureau of Labor Statistics 2005).

In those areas where there are extensive shortages of qualified workers, it is helpful to understand what motivates some older workers to continue working. One reason for a prolonged working career is a continued need to contribute to society and a desire to make a difference. A recent study from think tank Civic Ventures and the MetLife Foundation found that half of Americans ages 50 to 70 want jobs that contribute to the greater good now and in retirement. Various studies find that older workers are more likely to continue working when they have more control over their work hours, workplace flexibility, job autonomy and learning opportunities (MetLife Foundation/Civic Ventures New Face of Work Survey 2005).

Another reason people are working longer is financial need. A 2003 report from the Economic Policy Institute, a Washington, D.C. think tank, cited the loss of retirement wealth and the loss of access to retiree health insurance as causes for older workers to remain in the labor force longer than before. According to surveys by Watson Wyatt and others, many older workers, particularly those who opt for part-time work, look for companies that will "bridge" medical coverage until Medicare begins. Roughly one-third of the workforce continues to be covered under defined benefit plans. Moreover, because early retirement incentives are generally not incorporated into defined contribution plans, retirement rates among those in their early 60s have actually declined, reversing a decades-long trend (Gordon 2007).

Another strategy for managing a possible skilled labor shortage is to create a job bank of retirees that would like to be considered for part-time or full-time work after retirement. This could be used to match retiree skills with the demands of the university.

Health Aspects

Universities and colleges want the brainpower, experience, and knowledge provided by mature employees, but not the lost workdays, Workers' Compensation claims, or any of the negatives associated with injuries and illnesses. However, are the health-risk exposures of an aging work force as dire as some expect? If one considers the obesity, drug dependency, and anxiety levels of young people in general, they may not be much more physically fit than their elders in the workforce. According to the National Council on Compensation Insurance (NCCI) study, on average, younger workers have higher incidence rates of workplace injuries and illnesses than older workers, although older workers have higher costs per claim. A significant portion of the differences in claim severities between younger and older workers were accounted for by other factors correlated with age—average wages, claim durations, lump-sum payments, injury diagnoses, and number of medical treatments. The overall medical severity of lost time claims tends to rise for all age groups. Indemnity severity rises for all ages until age 65, when it falls due to Social Security offsets and lower average weekly wages (Shuford and Restrepo 2005). Also, there is not a consensus that older workers cost more to employ. For instance, the belief that older workers contribute to increased health care costs has been disproved by several studies. In particular, a research study by Yankelovich, Skelly, and White Inc. suggests that health care costs between three groups—30-year-old males, women with dependents, and 65-year-old retirees—are about the same. The study also concluded that 55-year-olds are the least costly of all groups. Moreover, results reveal that even if health care costs were higher, the advantages of employing mature workers virtually offsets any added cost because of lower absenteeism and turnover (Solomon 1995).

One unforeseen source for mitigating older worker health and safety risk exposures is the Americans with Disabilities Act. Because of such regulations, many employers have already modified public environments and will not have to make many additional drastic changes to meet the needs of mature workers. Some needed measures may include improving lighting, turning doorknobs into door levers, and building walkways that offer alternative ramps.

Mitigating the Health and Safety Exposure

Despite numerous studies challenging the perception that health and safety risk exposures increase drastically with an aging work force, the fact remains that our bodies change as we age. These changes are natural and can include: loss of strength, muscular flexibility, and joint

range of motion; diminished postural steadiness; reduced grip strength; change in balance, inner ear, and nervous system responses; reduced blood flow and tactile feedback; reduced visual capacity; and slowing of our mental processing (Pater 2006; Roth 2005).

As university risk managers, it is constructive to know what steps can be taken to reduce the frequency and severity of workplace accidents and illnesses for mature employees. In the area of risk identification, it is helpful to identify those jobs that possess the greatest physical risks (twisting of the upper torso, work with sustained fixed postures, etc.) through an organized, systematic process that is quantifiable. This will assist in prioritizing the jobs that need to be changed as well as those that could be used for return-to-work and to keep employees working longer.

While older employees have better safety records than younger ones in general, there are practical procedures employers can implement to improve workplace conditions and habits. Here are some suggestions:

- Reduce noise levels from machines, air conditioners and other appliances
- Ergonomically adjust seats and desktops at workstations to reduce leg and back problems
- Prevent long-term exposures to extreme hot and cold environments
- Prominently mark and light slippery floors, stairs, and uneven surfaces
- Set and enforce broad driver safety policies and evaluate jobs that require quick response times (According to the National Institute for Occupational Safety and Health, roadway crashes are the leading cause of occupational fatalities for older workers.)
- Post reminders about proper use of ladders to retrieve high objects and the use of carts or wheelbarrows for heavy lifting
  (Back pain is the leading cause of lost workdays and one of the most costly health problems facing employers today.)
- Recommend brief breaks from working at computers to avoid back problems and suggest hand exercises to reduce carpal tunnel syndrome
- Augment economy-of-motion training
- Promote memory training activities and a nutrient-rich diet for memory and attention
- Provide workers special keyboards to prevent carpal tunnel syndrome
- Use brighter lighting and larger type/screens on computer monitors to accommodate the loss of visual acuity (some conditions include presbyopia, a difficulty reading small print; floaters; and cataracts)
- Tactfully remind older workers to consider the reality of aging and recognize the changes in strength, agility, and balance that age inevitably brings, then adjust their work objectives to address those changes.

The belief that older workers contribute to increased health care costs has been disproved by several studies.

Stretching after work also keeps muscles flexible and reduces the risks of injuries. Aquatic therapy provides a reduced weight-bearing environment. Most universities and colleges have athletic facilities on campus that are available to employees, and many also offer various fitness classes on campus. Those that do not have on-campus facilities may consider investing in a discounted or subsidized membership fee for local YMCAs and health clubs. Sometimes a physician's prescription can assist in getting a reduced rate, too.

Another risk management issue that accompanies an aging employee base is the dreaded "slips and falls" exposure. According to the Liberty Mutual Research Institute for Safety, slips and falls are the second leading cause of workplace injuries. Same-level falls rank second in most industries (behind overexertion), and falls to a lower level rank fourth. The combined cost of slips and falls amounted to around $11.3 billion in 2004. As a broad generalization, aging workers are at a higher risk for slips and falls because they typically do not see as well, their muscles are not as strong for readily recovering balance, and their reflex time is sluggish (Minter 2004).

Given this reality, companies should be motivated to take a more proactive approach toward preventing slips, trips, and falls. Because of the variety of factors that can contribute to slips and falls, safety experts caution that

single remedies are far less likely to succeed than a comprehensive program that includes good design, maintenance, and training; slip-resistant footwear; accurate recordkeeping and reporting of close calls; evaluation of hazardous conditions, etc. Other areas that warrant even closer scrutiny are flooring and finishes, mats, floor coatings and treatments, and warning signs. Those responsible for safety and risk management should routinely audit the slip and fall prevention program to monitor the frequency and severity of slips and falls alongside objectives.

While these suggestions are certainly not comprehensive, they provide a good starting point to minimize injuries. Note that some of these modifications can also help younger workers stay healthier and safer, too.

Keeping Older Workers Happy and Productive

Sound management practices have proven over and over again that engaged employees show fewer signs of organizational neglect, such as absenteeism and less motivation. They even exhibit fewer aches, pains, and claims (Russell 2007). To ensure that the relationship between universities and their older employees remains mutually beneficial and productive, universities must take advantage of the knowledge and experience provided by older workers by involving them in innovations and procedure improvements. Everyone wants to be part of and contribute to organizational success.

Experienced older employees have much to contribute when they are included in the productivity process. In addition, studies have shown that a major cause of slowed mental function is, in fact, associated with lack of mind use or challenge. A survey conducted by the American Association of Retired Persons (AARP) asked respondents to rank attributes of the jobs they hold or plan to hold in retirement. Factors that contributed to a life/work balance and allowed workers to grow and learn new skills were deemed "very important" by half of those polled. A significant aspect of attracting and retaining older workers is offering them new roles and responsibilities, so they have a continuing sense of self-discovery (Mullich 2003).

A significant aspect of attracting and retaining older workers is offering them new roles and responsibilities, so they have a continuing sense of self-discovery.

Organizations should also continue to develop and train older workers. The Bureau of Labor Statistics reports that workers age 55 and older receive only one-third as many hours of formal training as workers 45 to 54. Reasons for these statistics may include the erroneous belief that "you can't teach an old dog new tricks," or the perception that some organizations do not want to waste time or money on employees nearing the end of their careers.

Fortunately, an increasing number of employers are beginning to make the connection between mature worker productivity and job attributes. Organizations are introducing flexible work schedules, retraining, health-and-wellness seminars, part-time positions, job sharing, and other strategies in an effort to retain and recruit older workers.

One other area that deserves mention is the relationship between mature workers and their younger counterparts. In some situations there are workers of retirement age with an active social life who have little interest in "moving up the ladder." Under those circumstances, it is not unusual to find supervisors or managers who are many years younger than subordinates. This appears to be more of an issue for the younger worker than the older worker, as younger managers sometimes feel like they are supervising their parents (or grandparents), and they feel uncertain of how to do so (Solomon 1995). However, when employers respect all employees and are consistent with their treatment, age becomes less of an issue. It is important to educate supervisors and managers on how to work with the Boomer generation, and to teach Boomers about the different generational attitudes toward work and authority.

Regulatory Compliance

Legislative and regulatory constraints may affect the ability of risk management programs to effectively deal with an aging work force. For example, rules from the Employee Retirement Income Security Act, the Internal Revenue Code,

and the Age Discrimination in Employment Act severely hamper true flexible retirement for most employees. There are legal ways to get around these norms, but it requires organizations to be creative and imaginative (Ruiz 2006).

Phased retirement has been an increasingly popular option in certain situations, such as with senior faculty members at universities. One difficulty that employers face when arranging a phased retirement plan centers on defined benefit (DB) pensions. These plans potentially complicate phased retirement in two ways. First, benefits sometimes depend on earnings in the last few working years prior to retirement. In those cases, an older person who chooses to work half time at half pay could lose as much as half of all future pension benefits. The second way in which DB pensions impede phased retirement involves federal pension regulations. However, a ruling last summer by the Internal Revenue Service provides guidelines that allow employers with DB plans to begin paying out benefits to employees age 62 or older, even if they continue working on a reduced schedule. For workers between 55 and 62 years old, employers are supposed to make a "good faith determination" of whether the worker is of "the normal retirement age" for the industry and can begin paying benefits to workers on a reduced schedule. The goal of these rules is to allow employers to retain workers longer.

The Social Security Administration also has rules that can affect early retirement benefits if an individual continues working while collecting Social Security. If one is under normal or full retirement age (FRA) when he or she starts getting Social Security payments, $1 in benefits will be deducted for each $2 earned above the annual limit. For 2007 that limit is $12,960. Remember, the earliest age someone can receive Social Security retirement benefits remains 62 even though the FRA is rising. In the year a person reaches his or her FRA, $1 in benefits will be deducted for each $3 he or she earns above a different limit, but only including earnings before the month FRA is reached. For 2007, this limit is $34,440. Starting with the month one reaches FRA, he or she will receive benefits with *no* limit on earnings. Note that another potential influence on the decision to continue working is the gradual increase in the full retirement age from 65 to 67 years of age.

Some universities have indicated that they may eventually adopt long-term incentive contracts for younger employees similar to those commonly used in private industry.

Aging Faculty

The graying of America's college and university faculty has occurred at roughly the same time as new federal regulations prohibiting mandatory retirement were enacted in the 1990s. Many current faculty members used student deferments during the Vietnam War to earn their graduate degrees, so the level of traditional retirement-age faculty is now substantial and continues to grow. Tenure, a senior academic's contractual right not to be fired without cause, can also complicate matters. While academic tenure is primarily intended to guarantee the right to academic freedom, it has been criticized for allowing some senior professors to become unproductive, shoddy, or irrelevant. About 50 percent of all U.S. colleges and universities have enacted a myriad of retirement incentives and processes to manage faculty retirements and assume more control over position vacancies (Leslie and Janson 2005).

Universities have been relatively unsuccessful in encouraging earlier retirements via pension plan and other incentives because these are expensive to offer faculty who are reasonably close to retirement. However, some universities have indicated that they may eventually adopt long-term incentive contracts for younger employees similar to those commonly used in private industry. Post-tenure reviews have also been implemented by a number of public and private universities to help underperforming professors get back on track.

Conclusion

While organizations understandably express health and productivity concerns about older employees, looming labor shortages are causing those same groups to seek out and retain older employees for their experience, accumulated wisdom, and work ethic.

It is important to remember that although some recruiting generalizations can be made about older workers, individuals in this group are as varied as any other large segment of the population. They include people who are in mid-life career changes, early retirees, older retirees, displaced workers, and people who have never worked outside the home before. Each group has its own motivations to work and benefits needs.

Many of these workers are eager to contribute to a university, if given the opportunity, and age does not seem to decrease creativity. A researcher recently made a list of the 1,000 most important ideas that had an impact upon the world, and the average age of the inventors was 74.

In addition to the health and safety suggestions mentioned, universities need to consider reviewing and amending their employee benefits where possible—especially retirement, pension and health care plans—in a way that facilitates retirees returning to work without being penalized. It is also imperative that university communications serve to invite older workers to come, stay, and work safely and productively.

About the Author

J. Tim Query, Ph.D., ARM, is a Baby Boomer as well as an Associate Professor of Risk Management and Insurance at New Mexico State University. He has research and consulting interests in various university risk management issues. Dr. Query wishes to thank NMSU graduate student Paul McHorse for his research assistance with this paper.

References

Bureau of Labor Statistics. "Labor Force Projections to 2014: Retiring Boomers." *Monthly Labor Review* (November 2005).

Gordon, Edward E. "Retiring Retirement: Mastering the Workforce Generation Gap." *Benefits & Compensation Digest* 44 (2007): 17–20.

Leslie, David W. and Natasha Janson. "Easing the Exit: An Aging Professoriate Likes Options." *Change* 37 (2005): 40–47.

MetLife Foundation/Civic Ventures, 2005, "New Face of Work Survey."

Minter, Stephen G. "Underestimating Slips and Falls." *Occupational Hazards* (October 2004).

Mooney, Sean F. "Aging Baby Boomers Impact Workers' Comp. Costs." *National Underwriter/Property & Casualty Risk & Benefits Management* 101, no.12 (1997).

Mullich, Joe. "They Don't Retire Them, They Hire Them." *Workforce Management* (December 2003): 49–54.

Pater, Robert. "Boosting Safety with an Aging Workforce." *Occupational Hazards* (March 2006).

Roth, Cynthia L. "How to Protect the Aging Work Force." *Occupational Hazards* (January 2005).

Ruiz, Gina. "Age Wave: Adapting to Older Workers." *Workforce Management* (March 2006): 32–36.

Russell, Rob. "Riding the Gray Wave." *Occupational Health & Safety* 76 (2007): 16–18.

Shuford, Harry and Tanya Restrepo. "Thinking About an Aging Workforce—Potential Impact on Workers Compensation." *NCCI Research Brief* 1 (May 2005).

Solomon, Charlene Marmer. "Unlock the Potential of Older Workers." *Personnel Journal* 74, no. 10 (October 1995).

What a paradox appears their age,
How people respond to them, yet know them not,
How there is something relentless in their fate all times,
How all times mischoose the objects of their
adulation and reward,
And how the same inexorable price must still be paid
for the same great purchase.

—Walt Whitman (1819–1892), "Beginners," *Leaves of Grass*

Above yon sombre swell of land

Thou see'st the dawn's grave orange hue

With one pale streak like yellow sand,

And over that a vein of blue.

—Richard Henry Horne (1803–1884), "The Plough"

The Threat Level Is Orange

Leta C. Finch, Executive Director of Higher Education Practice, Arthur J. Gallagher Risk Management Services, Inc.

Abstract: Risks are everywhere—the question is, which are possibly the most threatening and why? From the fluctuating climate, to mysterious viral mutations, to increasing unease over fuel shortages, this article presents some of the most pressing concerns that could soon affect risk managers everywhere.

The English historian, H.A.L. Fisher, wrote in 1935 in *A History of Europe*, "I can see only one emergency following upon another as wave follows upon wave."[1]

This paper presents eight potential crises that, were they to materialize, would present unprecedented challenges to risk managers. To minimize the destructive impact of each demands innovation in management techniques, new technology, and creative thinking. There are five threat levels as defined by Homeland Security: the lowest is green and the highest is red. For airline safety, the current level is orange or "high"—one step away from red, the most severe level possible.

Homeland Security defines five threat levels . . . the lowest is green and the highest is red.

In establishing the threat levels, the Attorney General, in consultation with the Director of the Office of Homeland Security, verifies the threat conditions using a variety of factors, including available evidence that can provide the answers to the following questions:

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- How grave is the threat?

The following risks are emerging in severity, complexity, and frequency, and for each the threat level is already high. Several are new and several have been around a while, but the magnitude of their impact is expanding significantly.

1. The effects of climate change
2. The increased numbers and spread of infectious and zoonotic diseases[2]
3. International travel incidents resulting in injuries, fatalities, and kidnappings
4. Terrorism, including acts involving nuclear, biological, chemical, and radiological (NBCR) weapons
5. Increased substance abuse
6. Increased campus violence
7. Increased student suicides
8. Oil shortages

How real are these threats to college and university campuses?

1. Climate Change

There is little doubt these days that climate change is occurring. Experts now agree that human-generated greenhouse gases are affecting the stability of the earth's weather patterns.[3] Nontheless, there are those who argue that because climate change has occurred throughout history, there is little to worry about. As reported in *The Economist*,[4] what may not be understood is that extreme weather fluctuation stopped about 10,000 years ago, and the climate settled down to what we have typically experienced since. Greenhouse gases, resulting from human activity, are at their highest in at least 650,000 years, and they continue to rise at an exponential rate.

These gases come from burning fuels and solid waste, agriculture and waste decomposition, and industrial processes.

A combination of rapid population growth (about 80 million net growth per year globally) and massive industrialization in countries like China and India are accelerating greenhouse gas production.[5]

Furthermore, climate change is making weather less predictable. In the last five years, for example, there have been a record number of destructive hurricanes, more frequent deadly heat waves in Western Europe and the

United States, and unprecedented severe flooding in many countries of Western and Central Europe.[6] As ocean temperatures rise, conditions for more hurricanes, typhoons, and other types of gale force windstorms will increase and hurricane seasons will last longer. Forest fires are expected to increase, more droughts will affect agriculture, and soil erosion from deforestation and flooding is expected to increase and reduce the ability of the ground to absorb water, also affecting crop yields.

The insurance industry sees these results of climate change as a threat to its viability, and as a result is taking natural catastrophe trends seriously.

In particular, Lloyd's of London has taken a lead in warning about the insurance consequences of climate change. Posted on their website is the following statement:

> We foresee an increasing possibility of attributing weather related losses to man-made climate change factors. This opens the possibility of courts assigning liability and compensation for claims of damage. . . .[7] We need to take action now and start discussing the steps we should take as an industry to prepare for the impact of climate change. It's a case of adapt or bust.

Climate change means exposures are changing, and new ones emerging.

Lloyd's has identified the following key issues for the insurance industry:

- "Climate change means exposures are changing, and new ones emerging. Insurers must regularly review and communicate conditions of coverage."
- "Recent events have shown capital and pricing models to be wanting. We must regularly update and recalibrate our models to keep pace with reality."
- "Insurers must prepare for the impact of climate change on asset values. Underwriting for profit will be key."
- "Effective partnership with business and government will be key to managing risk."

Risk managers can expect underwriting to be more aggressive in areas where the effects of climate change are expected to be particularly damaging to property risks.

2. Infectious and Zoonotic Diseases

Dr. Paul Hunter, head of health protection at the University of East Anglia in England, has presented research[8] indicating that there is strong evidence that climate change is contributing to the increased spread of infectious disease occurring around the world.

For example, illness-causing organisms that only grow in warm waters, such as those in the Gulf of Mexico, have now been reported as far north as the Baltic Sea. Congo Crimea Hemorrhagic Fever has also begun to appear in areas where it was previously unknown.

A mosquito-borne disease that was first detected in Central Asia and Africa and has since spread across the North American continent is the West Nile Virus (WNV). The CDC has reported that over 15,000 people in the United States have tested positive for West Nile infection since 1999, of which there have been more than 500 deaths.

As of July 2007, WNV infections have been reported to the CDC from Arkansas, California, Florida, Idaho, Illinois, Indiana, Iowa, Mississippi, Missouri, Nebraska, North Dakota, Ohio, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Virginia. (Note: not all states have WNV detection and reporting programs.)[9]

Another mosquito-borne disease of even greater concern to the CDC is Dengue Fever (DF). DF is now a pandemic and its global reach is comparable to malaria. From 1977 to 2004, a total of 3,806 suspected cases of imported DF were reported in the United States by travelers. Most fatal cases are among children and young adults.[10]

Recent news has made almost everyone aware of untreatable tuberculosis (TB), and the World Health Organization (WHO) has reported there are more than a few emerging strains that are drug resistant.

Currently, most of the 425,000 drug-resistant TB cases are occurring in the former Soviet Union, India, and China. However, four percent of all U.S. TB cases in the last year were drug resistant. There are about 1.7 million deaths per year worldwide from untreatable TB.[11]

A growing medical problem among athletes is Methicillin-Resistant Staphylococcus Aureus (MRSA), a highly contagious bacteria that causes blood infections, pneumonia, and, in some cases, death.[12]

MRSA is described as a "super bug" resistant to most standard antibiotics. The CDC has identified it as an emerging health risk because the number of "community-acquired" cases has increased. The spread among athletes is through contact sports, and it can exist anywhere there is crowding, poor hygiene, and broken skin.

According to *The Chronicle of Higher Education*,[13] in the past three years, outbreaks have occurred among sports teams at the following schools:

- University of Southern California
- University of Georgia
- Bowdoin College
- Lycoming College (PA) (where one player died)
- University of Tulsa (where one player died)

Antibacterial cleaning of gyms and locker rooms has cost these schools from $5,000 to $10,000.

A concern these days to almost every college and university is the threat of a pandemic flu outbreak.

At this point in time, all of the world's leading experts and public health officials agree that a pandemic flu outbreak is inevitable—the question is when.

Currently, the H5N1 virus (a subtype of the influenza A virus) has a 61 percent fatality rate,[14] primarily among the young and healthy. By comparison, the 2005 flu season had a less than 10 percent fatality rate primarily among the aged and ill.[15]

When an outbreak will occur depends on when it finally mutates into a strain that is easily transmissible from human to human. The mutation process of the virus is carefully monitored by the World Health Organization in every country where the virus has appeared. WHO is the appointed watchdog agency and will alert countries when an outbreak appears inevitable. Many colleges and universities have already begun developing response plans to cope with a predicted absentee rate of staff and faculty of approximately 30 per cent during the duration of the pandemic.

Below are reasons the Centers for Disease Control suspect for the global emergence of certain infectious diseases.[16]

Climate Change

As countries with cold and temperate climates warm, they become susceptible to the types of infectious agents typically found in tropical environments.

Increased Population Growth

Throughout the world, there has been urbanization and population growth. Often these changes have resulted in substandard housing, as well as inadequate water, sewer, and waste management systems, all of which can facilitate the growth and transmission of infectious diseases.

Poor Public Health Infrastructure

In many regions of the world, a public health infrastructure either does not exist or has deteriorated because of internal strife and war, or financial collapse. Many countries are barely able to respond to ongoing epidemics, leaving no resources available to develop disease prevention programs.

Increased air travel

Air travel has provided an ideal way by which infected people can transport infectious disease among the world's most populated cities.

Microbial Mutations

The rapidity with which many infectious microbes can mutate and adapt to change has led to the development of new, virulent strains that, in some cases, have developed drug resistance.

In a study by the Insurance Information Institute (III), the effects of a-million-plus death claims resulting from a pandemic would most likely include dramatic increases in reinsurance rates. Primary insurers would either be unwilling or reluctant to write new life and health polices.[17]

In addition, insurance regulators are already concerned about the possibility of insolvencies in the event of a pandemic flu outbreak and the need to reconsider risk-based capital requirements while there is time to do so.

Other concerns include uninsurable business interruptions as a result of having a large percentage of employees unable or unwilling to come to work during a pandemic. Parents with dependent children at home would most likely stay home with them as day care centers and schools close.

There will likely be significant delays in claims processing as insurers will also suffer from employees too ill or too afraid to show up for work.

There is additional concern that employers could experience liability claims from allegations of being

unprepared for a pandemic that they had sufficient warning about.

When the III released this information, it was meant to specifically address the insurance issues related to pandemic flu outbreak. The concepts are easily applicable to other types of infectious disease outbreaks.

3. International Program Risks: Illnesses, Fatalities, and Kidnapping

The goal of the Senator Paul Simon Study Abroad Foundation Act of 2007 (H.R. 1469, S.991) is to have one million students (approximately half of all U.S. college students graduating annually) acquire foreign language skills and international knowledge through expanded study abroad opportunities.[18]

Increasing the number of students studying abroad ensures a greater number of serious accidents and illnesses occurring while in a foreign country. For example, more students will be exposed to car accidents, muggings and assaults, infectious diseases, acts of terrorism, substandard healthcare facilities and non-western trained providers, and kidnappings and ransom demands, to name a few.

Kidnapping in particular is a growing risk with estimates of 20,000–30,000 persons kidnapped annually.[19] In many developing countries, kidnapping gangs exist because of the financial incentive from paid ransoms.

The countries that create the greatest kidnapping risks are those with the largest gaps between the wealthy and poor (with little to no middle class, resulting in significant income distribution problems); countries with ongoing internal conflicts; and countries in which the governments are highly corrupt. According to The World Bank, there are 71 countries that meet this description.[20] Most of these countries appeal to students, and faculty members are willing to take them there.

4. Terrorism and NBCR releases

The threat of terrorism using nuclear material is particularly challenging to minimize. A database kept by the United Nations organization, the International Atomic Energy Agency (IAEA), reveals that worldwide since 1993, there have been 16 confirmed cases where "highly enriched uranium or plutonium (of which both can be used as the core of a nuclear weapon) has been lost, stolen, or seized from would-be traffickers."[21] The story goes on to state that not all countries bother to report such incidents, and, thus, it can be assumed many more such events have occurred.

The threat of terrorism using nuclear material is particularly challenging to minimize.

Consider this scenario:

According to the Rand Corp, as reported in *Risk Management*,[22] a 10-kiloton nuclear bomb detonated in a shipping container at a Long Beach, California, port would cause "10 times the economic damage" of the World Trade Towers attack, and destroy a significant area of metropolitan Los Angeles, killing 60,000 people. Another 150,000 people would be exposed to hazardous levels of radiation, and another two to three million people could be forced to move out of the extended area because of the potential for nuclear contamination.

Resulting fires from the blast could potentially destroy all of the ships and existing infrastructure of the port, including the Los Angeles port. Some areas near the epicenter would not be habitable for at least 20 years. The economic impact would be felt worldwide and worsened if the United States chose to close all ports as a temporary security precaution.

Combined, Long Beach and Los Angeles, California's shipping ports, handle one-third of all imports into the country.

How probable is this event?

As Daniel Benjamin and Steven Simon, two former U.S. counter-terrorism officials, noted in the journal *Foreign Affairs*, "All that is needed for a terrorist attack to succeed are the most portable, least detectable tools of the terrorist trade: ideas." [23]

Nuclear, biological, chemical, and radiological (NBCR) agents can be spread by numerous means, for example through HVAC systems, food and water supplies, crop dusters, and, of course, the U.S. Postal Service.

Money is no inhibitor to terrorism, either.[24] John Muller, in the September/October 2006 edition of *Foreign Affairs*, wrote that it is estimated that Al Qaeda's

September 11 attack on the World Trade Towers cost less than $500,000 to execute.

The April 2004 Madrid subway bombings cost less than $1,000, and were later replicated in London and Mumbai. For close to $1,000, an Al Qaeda affiliate killed 200 people in a nightclub bombing in Bali.

In his book *Terror and the Internet: The New Arena, the New Challenges*, Gabriel Weimman points out that in his eight-year study of terrorists' use of the internet, he found 40 organizations designated as active terrorist groups by the U.S. State Department that maintain over 4,000 websites.[25]

Terrorists use the internet to:

- Solicit money
- Recruit new supporters
- Distribute training and weapons-making materials
- Gather information about future targets.

Unfortunately this threat will not abate anytime soon, and perhaps not in the foreseeable future. Insurance will remain elusive and expensive at best. And coverage for events involving NBCR agents is not available, with most of the insurers opposing offering any such coverage.[26] As stated in the May 25, 2007 edition of *Business Insurance*,[27] "NBCR events are qualitatively and quantitatively different from events arising from the use of conventional terrorist weapons."

5. Increased Substance Abuse

Almost every college and university in the United States has by now had to address the issue of substance abuse on their campuses. This can include underage drinking and binge drinking of alcoholic beverages, use of illegal drugs, and overuse of prescription drugs. Every year, students die from such abuse.

The impact and uninsurable costs of incidents involving student substance abuse include increased aggressive behaviors resulting in physical injury and property damage, poor academic achievement of those involved, and damage to the institution's reputation when incidents of substance abuse are severe.

Almost every college and university in the United States has by now had to address the issue of substance abuse.

The Substance Abuse and Mental Health Services Administration, a division of the Department of Health and Human Services, conducts an annual national survey on drug use and health. SAMHSA creates "TEDS," the Treatment Episode Data Set.

TEDS identifies "youth" as those persons whose ages are between 12 and 17, and "young adults" as those persons whose ages are between 17 and 25.

The 2005 TEDS data set (the most recent available as of this writing) indicated the following:

- 1.5 million youths (six percent of the youth population) were classified as needing alcohol treatment, and only about seven percent received it.
- About an equal number of youths were classified as needing illicit drug use treatment, and nine percent received it.
- The criminal justice system was the principal source of referral to substance abuse treatment for 47 percent of young adults (ages 17–25), and for 52 percent of youths.
- Based on the TEDS supplemental data set, 17 percent of young adults had a psychiatric problem in addition to substance abuse, as did 20 percent of the youth admissions for substance abuse treatment.

The situation is worsening.

In 2006, Afghanistan had a record crop of opium (the source of heroin) with a 60 percent increase over the previous year. In 2007, the crop yield set another record. Acreage harvested that year for opium was 457,135 compared with 407,715 acres in 2006. Afghanistan now produces 90 percent of the world's opium, and as a result, the availability of heroin has recently outstripped demand. It is now cheaper and more easily available.[28]

Where does this lead us?

6. Increased Campus Violence

According to SAMHSA, the National Survey on Drug Use and Health indicated that youths ages 12 to 17 who used alcohol and/or an illicit drug in the past year were almost twice as likely to have engaged in a violent behavior

as those who did not use alcohol or an illicit drug (49.8 percent versus 26.6 percent).

Too many colleges and universities have had to manage the aftermath of the worst situation imaginable—a person's violent madness taken out on innocent members of the campus community.

Two important considerations:

- Homicide (mostly from guns) is second only to vehicle accidents as the leading cause of occupational death in the workplace in the United States for women.[29]
- Persons who have experienced a lifelong exposure to violence and illegal substances are becoming members of our higher education staff, faculty, and student communities.

Cases of violence on campus have involved staff, spouses of staff and faculty, and outsiders, but most cases reported in the general media have involved students as the perpetrators.

Virginia Tech, the most recent and most horrific example, is but one in the history of cases of violence by students on campus.

Although an act of violence has occurred on a college or university campus every year now for decades, 2002 was particularly violent. That year, at the University of Arizona's College of Nursing, three professors were shot to death by a student, and similar to Seung-Hiu Cho at Virginia Tech, the student later committed suicide. Another student at the Appalachian School of Law shot and killed the law dean, a faculty member, and a student. And a fight between students at Catawba and Livingstone Colleges in Salisbury, North Carolina, resulted in gunshots that left a Catawba student dead and six Livingstone students charged with homicide.

Although the shooting spree that Dylan Klebold and Eric Harris embarked upon in 1999 was not on a college or university campus, what they accomplished at Columbine High School could have been considered foretelling at the time. Based on statements made by Dylan Klebold's parents that they were completely unaware of their son's intent to commit murder and suicide, Professor Garbarino of Cornell University and the author of *Lost Boys: Why Our Sons Turn Violent and How We Can Save Them*, wondered how that could be.

The fall 2002 edition of the magazine of the Harvard Graduate School of Education reported in an article titled "The Secret Lives of Adolescents"[30] that Professor Garbarino asked his students to research the question, "Is it possible for parents to fail to see murderous and suicidal tendencies in their children?" The study found that many teens admitted to having been raped, tried illegal drugs, committed acts of vandalism, and seriously considered suicide. The respondents believed that their parents knew nothing of these events or behavior.

Acts of anger and aggression are often drug induced. According to SAMHSA's, 1999 National Household Survey on Drug Abuse, an estimated 833,000 youths between the ages of 12 and 17 had carried a handgun in the past year.

Virginia Tech is but one in the history of cases of violence by students on campus.

According to the national survey of crime victims, the rate of firearm violence increased in 2005. We are likely to see this situation worsening.

7. Increased Student Suicides

As reported in SAMHSA's 2004 National Survey on Drug Use and Health, an estimated 2.2 million adolescents aged 12 to 17 have experienced at least one major depressive episode during the preceding year. Depressed adolescents are more than twice as likely to have used illicit drugs as their peers who had not experienced a major depressive episode.

Consider that an estimated 712,000 adolescents had tried to kill themselves during their worst or most recent major depressive episode (representing almost three percent of those ages 12 to 17). Only 36 percent of youths at risk for suicide during the past year received mental health treatment or counseling. A portion of this age cohort arrives on college and university campuses every fall.

The 2006 American College Health Association's National College Health Assessment reported that the number of college students who said they had ever received a diagnosis of depression increased by 4.6 percentage points over the last four years. Of the students

who reported a diagnosis of depression, 38 percent said they were taking medication for it and 25.2 percent said they were in therapy.

In addition to those statistics, about 10 percent of all students surveyed in 2004 said they had seriously considered suicide at least once during that year.

Based on the numbers of youths and college students at risk, we can expect to see a growth in the number of student suicides on campus and, considering the liability issues, colleges and universities had better be prepared to do all that is possible to prevent them from occurring.

8. Oil Shortages

As if everything else risk managers are facing is not challenging enough, the most difficult may be the impending oil crisis.

In their CEO briefing, *The Economist*'s Intelligence Unit reported that their survey of 500 CEOs revealed that managing the scarcity of oil was one of the major challenges identified in the upcoming decade. What is the basis for this concern? The United States is heavily dependent on oil, the growing shortage is affecting the cost of doing business, and there are few effective and affordable alternatives available in mass quantities.

In 1956, Shell oil geologists predicted that the domestic oil production would peak between 1965 and 1970. It peaked in 1970.[31] At the same time it was predicted that global oil production would peak in the year 2000. Although that has not happened, pessimists believe that the world peak may occur as soon as 2011, and optimists believe we have another 30 years before the peak. Whatever the case, no one disputes the fact that petroleum, the source of fuel oil, is a limited resource and that a peak is inevitable.

Bryant Urstadt wrote in *Harper's* August 2006 edition a piece titled "Imagine There's No Oil" which noted that more than half all of the remaining oil in the world is in the Middle East. The United States owns about five percent of the remaining world oil reserves, but it is estimated that we consume within U.S. borders 30 percent of all the oil produced in the world.

Based on the numbers of youths and college students at risk, we can expect to see a growth in the number of student suicides on campus.

In addition, China is gaining in oil consumption. Since 2000, Urstadt observed, China has accounted for one-third of the increase in world oil consumption. China has 13 million car owners today, whereas in 1995, they only had two million.

Worldwide consumption does not appear to be decreasing at a rate to delay the anticipated oil peak. Nevertheless, according to Noam Scheiber in "Where the Oil Is," an article published in *New York Times Magazine* on November 10, 2002, there are, however, untapped reserves in countries such as Russia, Kazakhstan, and Azerbaijan, and improvements in technology could result in more efficient extraction processes in West Africa and the U.S. Gulf Coast.[32]

Latin America could increase its production. Colombia, however—once a major exporter of oil—has experienced frequent attacks on its pipeline. In 2005, the United States had to invest $100 million in counterinsurgency aid to keep a major U.S. oil company from leaving Colombia.[33]

Many offshore oil sites are in deep-water fields with considerably higher extraction costs.[34]

Nigeria could supply the United States with more oil, but the political situation is unstable and kidnappings of oil workers have significantly decreased production.[35]

As Urstadt wrote in *Harper's*, life without oil is bleak.[36]

- Starvation will be more widespread because food production and transport is oil dependent.
- Wars will occur more frequently over scant remaining oil. Fighting over limited resources is already happening in countries in Africa.
- Dirty alternatives like coal will affect climate change.
- Cars may become luxuries because of limited production of alternative fuels.
- Production of plastics will cease as plastic is derived from petrochemicals.
- Consumer goods will become unaffordable or unavailable, as they are typically shipped to their destination at large energy costs.

- Many buildings will not be heated or cooled.

There are alternatives, but each creates it own challenges, risks, and production limitations. Urstadt summarizes for his readers issues with each of the alternative fuels.

Coal

As a fossil fuel, burning coal has a huge impact on global warming. More burning will only increase the effects.[37]

Nuclear Power

Today there are 103 nuclear power plants in the United States. To replace today's oil consumption, with no increase in energy use, the United States would need 427 more plants,[38] and that is without providing any power for cars. Nuclear waste remains the biggest problem for society to solve.[39]

Alternative Fuels

Corn grain ethanol and soy biodiesel currently provide six percent of our total energy needs. To grow enough biomass to meet today's world energy needs would require more than 10 percent of the world's landmass, approximately all of the land that is already under cultivation. Furthermore, we would have to cultivate new landmass and transport the crops using machinery that does not use petroleum.[40]

Also consider that current production processes of ethanol and soy biodiesel consume only slightly less energy than they produce. Burning ethanol results in only 12 percent less greenhouse gas emissions than burning gasoline. Soy biodiesel provides a 41 percent reduction in greenhouse gases; however, with current technology, one acre of soybeans yields only 60 gallons of fuel.[41]

Solar

For solar and wind power to equal the output of one nuclear power plant, one would need to build five square miles of solar panels or turbines.[42]

Geothermal Power

Geothermal power is renewable, but it can only be used close to its source.[43]

Electric Cars

Electric cars are currently usually powered by energy from non-renewable sources.

Hydrogen

Hydrogen is far more expensive to produce than gasoline, and a single hydrogen-powered car costs hundreds of thousands of dollars.

There is an urgency to find new reserves, and research and development is occurring. In the meantime, the cost of gas continues to escalate, grain products like cereals are soaring as food grains are diverted to biofuel production (increased demand for ethanol has already resulted in a doubling of the price of corn in the last year[44]), and the cost of doing business will begin to affect personal incomes.

No one disputes the fact that petroleum is a limited resource and that a peak is inevitable.

Conclusion

In 2006, as a result of diverse and complex changes occurring in the world and the impact these changes have had on insurers, the United Nations' Environment Programme Finance Initiative created the Insurance Working Group (IWG), consisting of 16 insurers, reinsurers, and brokers from Australia, Bermuda, France, Germany, Greece, Japan, Norway, Spain, Sweden, Switzerland, the Netherlands, the United Kingdom, and the United States.[45]

The IWG's inaugural report on sustainability stated, "Climate change is the greatest environmental risk confronting the insurance industry, but it is not the only one."[46]

Although this paper reports on many of the challenges risk managers must now consider addressing on their campuses, there are still others that have gone unmentioned. Simply, the number of concerns and dangers in the world are limitless. Yet it is all too easy to become ostrich-like and bury one's head. The most vexing problem about the risks described in this paper is that, in many cases, the threats are vague. This in itself creates a bigger risk. In the book *Facing Ambiguous Threats*, authors Roberto, Bohmer, and Edmonson state, "The most dangerous situations arise when the threat is ambiguous. This leads managers to ignore or discount the risk and take a wait-and-see attitude. Such an approach can be catastrophic."[47]

We can also become anchored to an opinion, causing us to underreact to new information. Sometimes we have chosen to believe in something at any cost, becoming wedded to certain beliefs because we don't like or want to know the facts.[48]

Because one can easily become complacent about ambiguous risks, it is easier to believe such events would not or could not affect one's campus. To counter this thinking, Bob Bickel of the Stetson Law School has said that one must overcome the unconscious belief that the campus is safe. In other words, "the illusion of safety is its own kind of danger."

So what can risk managers do to begin to prepare their campuses for these emerging crises?

1. Get past fear and denial, and then urge top management to get past it, too. As risk managers know, it is far better to identify the risks, think logically, and plan ahead, than to be taken by surprise. Averting a crisis may not always be possible, but risk management steps are valuable in helping to minimize one and to recover more quickly; otherwise we can suffer from extreme regret after the event. A risk manager's job is to take steps to avoid such regret. As the old Chinese saying goes, "Take care of the difficult while it is still easy."
2. Realize that finding insurance solutions for any or all of the risks reported on in this paper is difficult at best, and in some cases, impossible. Where coverage may be available, a cost/benefit review by the institution of the exclusions and premiums may show that coverage is not advantageous.
3. With few insurance options available, there is a crucial need to minimize the potential catastrophic consequences of each of the risks identified. In other words:
   - Identify the threats that could affect your campus
   - Evaluate your institution's vulnerability to those threats
   - Evaluate the impact of these threats to your institution
   - Assess existing operating policies, procedures, and protocols intended to minimize potential threats and to manage a catastrophic event
   - Develop comprehensive response, recovery, and business continuity plans
   - Develop breadth and depth of awareness and response skills among all persons affiliated with your institution, and most importantly, with senior management.

This paper has not intended to summarize every new or emerging challenge facing risk managers. Rather, its intent is to clarify the need for urgency in preparing college and university campuses for the threats looming on the horizon. No campus is immune to them.

The greatest challenge, however, may be convincing senior management of the potential severity of these threats and the need to begin planning for them. Perhaps a final thought from R. Buckminster Fuller can help to inspire the planning process: "We are called to be architects of the future, not its victims."

About the Author

Leta Finch has more than 25 years of experience in higher education risk management, and formerly served as the Director of Risk Management at the University of Vermont. She also served as the Director of the Institute for Financial Services at Champlain College, where she was a member of the Dean's Council. Ms. Finch is a member of the Board of Trustees of Champlain College, and a member of the international board of directors of Samara State University in Samara, Russia. She has also served as a trustee of the American University of Central Asia. She is founder and president of the Foundation for Higher Education in Central Asia, past president of URMIA, and a recipient of URMIA's Distinguished Risk Manager Award. She received her bachelor's degree from the University of Hawaii and holds a master's degree in public administration from the University of Vermont.

Endnotes

1 Antony Jay, ed., *The Oxford Dictionary of Political Quotations* (Oxford: Oxford University Press, 1996), p. 136.

2 A zoonotic disease is one which normally exists in animals but that can be transmitted to and infect humans. There are many zoonotic diseases including anthrax, plague, Lyme disease, monkey pox, rabies, trichinosis, typhus and West Nile fever.

3 "A Dangerous Experiment," The Sierra club, Global Warming Fact Sheet, p.1.

4 "The heat is on," *The Economist,* September 9, 2006, p. 11.

5 "The heat is on," *The Economist,* September 9, 2006, p. 11.

[6] "What is Global Warming," *National Geographic,* Environment; http://green.nationalgeographic.com/environment/global-warming/

[7] Lloyd's 360 Risk Project, Climate Change: Adapt or Bust, p. 5 (report can be accessed at www.lloyds.com/360).

[8] BBC NEWS, http://news.bbc.co.uk/go/pr/fr/-/2/hi/science/nature/5311196.stm; published 2006/09/04.

[9] Communicated by ProMED-mail, promed@promedmail.org, the global electronic monitoring and reporting system for outbreaks of emerging infectious diseases and toxins, a program of the International Society for Infectious Diseases.

[10] Dengue Fever Fact Sheet, Centers for Disease Control, Department of Health and Services, January 7, 2005.

[11] Drug and Multi-Drug Resistant Tuberculosis (MDR-TB) Fact Sheet, World Health Organization.

[12] Erin Strout, "An Unwelcome Visitor in the Locker Room," *The Chronicle of Higher Education,* September 29, 2006, p. A46.

[13] Erin Strout, "An Unwelcome Visitor in the Locker Room," *The Chronicle of Higher Education,* September 29, 2006, p. A46.

[14] Cumulative Number of Confirmed Human Cases of Avian Influenza A/(H5N1) Reported to WHO; World Health Organization; 25 July 2007; http://www.who.int/csr/disease/avian_influenza/country/cases.

[15] Update: Influenza Activity—United States, 2004–05 Season; MMWR (Morbidity and Mortality Weekly Report), Centers for Disease Control, April 8, 2005.

[16] National Center for Infectious Diseases, Centers for Disease Control, website http://www.cdc.gov/ncidod/.

[17] Avian Influenza (Bird Flu), I.I.I. Research and Analysis, Insurance Institute of America.

[18] Public Policy: Senator Paul Simon Study Abroad Foundation Act of 2007; NAFSA: Association of International Educators (http://www.nafsa.org/public_policy.sec/study_abroad_2/faqs_2/#significance).

[19] "Risk Managing Kidnap and Ransom Exposures," *The Risk Report,* IRMI, April 1999.

[20] States and Markets, 2007 World Development Indicators, The World Bank, p. 260.

[21] *The Economist,* February 3, 2007, p. 60.

[22] "Effect of Nuclear Blast at Port Would Be National," *Risk Management Magazine,* October 2006, p. 8.

[23] John Mueller, "Is There Still a Terrorist Threat?" *Foreign Affairs,* Volume 85, No. 5, September/October 2006, pp. 3-4.

[24] John Mueller, "Is There Still a Terrorist Threat?" *Foreign Affairs,* Volume 85, No. 5, September/October 2006 pp. 3-4.

[25] Gabriel Weimman, "Terror and the Internet: The New Arena, the New Challenges," United States Institute of Peace Press; as cited in *The Economist,* April 29, 2006, p. 87.

[26] Mark Hofmann, "Industry groups says NBCR events 'uninsurable,'" *Business Insurance,* May 25, 2007.

[27] Mark Hofmann, "Industry groups says NBCR events 'uninsurable,'" *Business Insurance,* May 25, 2007.

[28] "Afghanistan will break opium growth record," Associated Press, July 18, 2007.

[29] National Census of Fatal Occupational Injuries in 2005, Bureau of Labor Statistics, United States Department of Labor; August 10, 2006, p. 12.

[30] "The Secret Lives of Adolescents," *ED,* the magazine of the Harvard Graduate School of Education, Fall 2002.

[31] Bryant Urstadt, "Imagine There's No Oil," *Harper's,* August 2006, p. 32.

[32] Noam Scheiber, "The Way We Live Now: Economics of Oil; Where the Oil Is," *New York Times Magazine,* November 10, 2002.

[33] Noam Scheiber, "The Way We Live Now: Economics of Oil; Where the Oil Is," *New York Times Magazine,* November 10, 2002.

[34] Noam Scheiber, "The Way We Live Now: Economics of Oil; Where the Oil Is," *New York Times Magazine,* November 10, 2002.

[35] Noam Scheiber, "The Way We Live Now: Economics of Oil; Where the Oil Is," *New York Times Magazine,* November 10, 2002.

[36] Bryant Urstadt, "Imagine There's No Oil," *Harper's,* August 2006, p. 34.

[37] "As Security and Climate Concerns Rise, Nuclear Power May Be Coming Back," *The Economist,* June 2, 2007.

[38] Bryant Urstadt, "Imagine There's No Oil," *Harper's,* August 2006, p. 32.

[39] "As Security and Climate Concerns Rise, Nuclear Power May Be Coming Back," *The Economist,* June 2, 2007.

[40] Bryant Urstadt, "Imagine There's No Oil," *Harper's,* August 2006, p. 40.

[41] Kevin Bullis, "Ethanol vs. Biodiesel," *Technology Review,* published by MIT, Sept/Oct 2006.

[42] Bryant Urstadt, "Imagine There's No Oil," *Harper's,* August 2006, p. 40.

[43] Geothermal FAQs, Geothermal Technologies Program, U.S. Department of Energy (http://www1.eere.energy.gov/geothermal/faqs.html)

[44] "Biofuelled: Grain prices go the way of oil prices," *The Economist,* June 23, 2007.

[45] Richard Miller, "U.N., Insurers Release Sustainability Report," *Business Insurance,* May 25, 2007.

[46] Richard Miller, "U.N., Insurers Release Sustainability Report," *Business Insurance,* May 25, 2007.

[47] Michael A. Roberto, Richard M. J. Bohmer, and Amy Edmonson, "Facing Ambiguous Threats," *Harvard Business Review,* November 2006, p. 110.

[48] Richard T. Zatorski, "Vividness, Anchoring, and Regret," *Contingencies,* September/October, 2000, p. 76.

I lived on dread; to those who know

The stimulus there is

In danger, other impetus

Is numb and vital-less.

—Emily Dickinson (1830–1886), "Time and Eternity"

Now I am terrified at the Earth! it is that calm and patient
It grows such sweet things out of such corruptions
. . . . It renews with such unwitting looks, its prodigal,
annual, sumptuous crops
It gives such divine materials to men, and accepts
such leavings from them at last.

—Walt Whitman (1819–1892), "This Compost," *Leaves of Grass*

Mold in the Environment: The Difficulty of Assessing the Risk

George H. Bender, Manager of Environmental Health and Safety, Duquesne University

Abstract: Mold can contribute to a variety of adverse health conditions, and it is often problematic because of its many manifestations. While some forms of mold are more dangerous than others (and at varying levels of exposure), a number require extensive procedures to detect, address, and prevent. This article analyzes various forms of mold, the health threats they pose, and subsequent strategies for risk managers who must deal with its changeability.

Introduction

Mold, or more appropriately fungus, is found everywhere in the natural outdoor environment. Its prime purpose is to break down organic material, and it has been known to man for thousands of years. Many believe that mold was first loosely referenced in Chapters 13 and 14 of the Book of Leviticus in the Bible.* But the first chronicled reaction to mold exposure is described as a serious outbreak of ergotism, a type of poisoning brought on by ingesting a certain fungus present in the Rhine Valley in 857 A.D. People suffered swollen blisters, rotting flesh, and loss of limbs, and the affliction was named the Holy Fire. In 1039, another similar episode of ergotism erupted, named St. Anthony's Fire. While the cause of both outbreaks was not known at the time, the details surrounding the events suggest mold was at fault.

The next documented occurrence of side effects from mold exposure was in 1670, when a French physician, Thuillier, observed that ergot was growing on grain stalks instead of grain. In the following years ergot was especially prevalent, and the incidence of St. Anthony's Fire increased dramatically. Still, the cause of the outbreaks was not recognized. Finally, in 1853, Louis Rene Tulanse proved that the fungus *Claviceps pupurea* was attacking rye grain and was the cause of ergotism. This fungus contained poisonous alkaloids that caused a variety of health problems when eaten by humans or animals. In fact, this species of fungus was the first source for lysergic acid diethylamide (LSD). As society became more civilized, the awareness of mold and its effects became more prevalent. Many people have even theorized that the Salem Witch Trials held in 1692 were the result of ergotism suffered by women. Although outbreaks of ergotism have occurred since 1853, the last reported case was in 1951 (University of Georgia 2005).

In the 1990s, the unhealthy side effects of mold returned to the forefront. Between 1994 and 1997, 10 infants in Cleveland were identified with acute idiopathic pulmonary hemorrhage, also called pulmonary hemo-siderosis. It was theorized that the affliction was due to the infants being exposed to the fungus *Stachybotrys chartarum (S. chartarum)* six months before the onset of illness, through inhalation. *S. chartarum* is known to grow indoors in moist environments and produce mycotoxins that are toxic (Dearborn et al. 2002; Centers for Disease Control and Prevention 2000).

In the 1990s, the unhealthy side effects of mold returned to the forefront.

In late 1999, an article published in *USA Weekend* described the problems that a woman named Melinda Ballard and her family were having with *S. chartarum* in their new home. The copper plumbing in the home began to leak in 1998, and by December, the hardwood floors began to warp. By March 1999, the entire family was experiencing a series of health problems, which became so severe that the family was forced to vacate the home and live in a nearby motel. The ensuing lawsuit filed by Ms. Ballard resulted in a multimillion-dollar award to her and her family (Mann 1999).

As a result of the Cleveland infants and the Ballard case, the media began to increase the reporting about *S. chartarum* or the "toxic black" mold and the harm it could cause. Naturally, this heightened public awareness

raised concerns about exposure to mold indoors. These concerns have contributed to the development of a service market to evaluate the risk associated with exposure to molds or fungi (Flappan et al. 1999).

Initially, risk assessment generally involved a four-step process: hazard identification (health effects), exposure assessment, establishment of a dose-response relationship, and finally the assessment of the degree of risk (DiNardi 1997). To date, this process appears to be more of a subjective effort than an objective one, placing professionals in a position of having to conduct risk assessments for an exposure for which there is limited scientific information or consensus for support. The following reviews the current information available as it applies to the risk associated with fungal exposure and describes the difficulty involved in determining that risk.

Health Effects

Approximately 1,000 species of mold or fungi can be found in the United States, and more than 100,000 species have been identified worldwide (United States Occupational Safety and Health Administration 2003). They typically affect human health adversely in three ways: allergy, infection, and toxicity (Robbins et al. 2000). Molds that are generally found outdoors are of more concern than those found indoors because they cause airway allergic diseases such as allergic asthma or rhinitis. Red eyes and a runny nose are the most common allergic responses observed. These responses are the result of the body producing allergic antibodies (IgE) to address the "attack" of fungal spores or hyphal fragments inhaled into the lungs. Although 40 percent of the population displays high levels of allergic antibodies in their systems, only five percent actually present allergic symptoms (Hardin et al. 2003). *Aspergillus* and *Penicillium* species are associated with the indoor environment, while *Cladosporium* and *Alternaria* species are affiliated with the outdoors. These outdoor species are believed to be the cause of airway allergic disease—more so than indoor species. However, exposure to bacteria, dust mites, and endo-toxins will also elicit the same reactions as fungi or molds. Each could contribute to the overall "illness," but the exact contribution of each is unknown.

Molds that are generally found outdoors are of more concern than those found indoors.

Another health effect is hypersensitivity pneumonitis (HP), which is an inflammation of the alveoli. It is not induced by normal or slightly elevated concentrations of mold propagules, but instead is a result of the body producing excessive IgE antibodies in reaction to exposure to molds. Although most cases result from occupational exposures, some cases have been attributed to birds, humidifiers, and HVAC systems. Thermophilic actinomyces, which are bacteria rather than fungi, are the organisms associated with exposures from humidifiers and HVAC systems.

Allergic bronchopulmonary aspergillosis (ABPA) and allergic fungal sinusitis (AFS) are variations of allergic reactions in which the fungi actually grow in the airways. In both cases, patients have preexisting airway damage that impairs normal drainage. This permits the fungus to grow without affecting any adjacent tissue. Usually this does not result in any health issues unless the patient is allergic to the specific fungus. Although *Aspergillus* is the fungus typically involved, *Curvularia* is also associated with AFS.

With regard to infection, there are a limited number of fungi, particularly indoors, that can infect humans internally and possibly cause death. *Cryptococcus* (bird droppings), *Histoplasma* (bat droppings), and *Coccidioides* (soil from southwest United States) are generally not found indoors and are pathogenic only to people who are immunocompromised.

Skin and mucosal infections, on the other hand, are quite common and involve the feet, nails, groin, skin, and oral or vaginal mucosa. Moisture in shoes, body creases, and loss of epithelial integrity are critical to this type of infection. But it should be noted that the fungus *C. albicans* might be found on half of the population that exhibits no sign of infection.

Yet another health effect of mold is caused by mycotoxins, which are secondary metabolites that result in mold toxicity. How mycotoxins are produced is not clearly understood; therefore, the presence of a toxigenic mold does not mean that mycotoxins are present. Instead, production is dependent upon nutrient availability,

temperature, and humidity. When mycotoxins are produced, they are found in all parts of a fungal colony. Typically in the past, exposure has been the result of the ingestion of contaminated foods. The other method of exposure is inhalation, but few studies have researched the inhalation of mycotoxins, which is the primary source of infection in today's society (Robbins et al. 2000).

Molds, furthermore, do not produce the same mycotoxins. *Aspergillus* species, for example, produce the mycotoxin aflatoxin, whose ingestion has been related to liver cancer. Some *Penicillium* species produce the mycotoxin ochratoxin A, which is teratogenic. On the other hand, *Alternaria* produces a wide array of mycotoxins. Skin irritation, vomiting, diarrhea, hemorrhage, convulsions, and sometimes death are the result of exposure to trichothecenes, which are mycotoxins produced by some molds, particularly *Fusarium* species.

Mycotoxins themselves produce volatile organic compounds (VOCs) that can be inherently toxic. But the concentration of VOCs produced is not toxic by inhalation—it would require one to inhale an extremely high concentration not found in homes, offices, or schools (Kelman et al. 2004).

Glucans, which are glucose polymers that are located in most fungal cell walls, are often associated with mycotoxins. It is believed that they play a role in some fungal infections, particularly hypersensitivity pneunomitis, by affecting airway macrophages. Exposure is determined by bioassays, but it is generally assumed that if you are exposed to fungi, you are exposed to glucans (Macher 1999).

Exposure Assessment

Visual Inspection

Before an exposure assessment strategy can be developed, a visual inspection of the affected building or area is required. Fungal growth requires moisture, a food source, and the proper temperature. Therefore, the inspection should involve, in addition to quantifying visible fungal growth, the identification of water intrusion, including dampness, water leaks, or flooding, and damaged cellulose-based building components. The fungal growth must also be quantified, since this is a measure of the extent of possible contamination. Occupant behavior must be noted, as well. Some additional indicators of possible fungal issues include poor maintenance of HVAC equipment, storing firewood indoors, poor housekeeping, and attaching greenhouses to buildings. Assessment of certain odors can be helpful too, as they may be an indication of hidden fungal growth. For example, a "musty" odor is the result of the production of VOCs from normal growth, while a "dirty sock" odor is indicative of bacterial growth. Chemical odors may also contribute to respiratory problems and need to be considered (Dillon et al. 1999).

Questionnaires

Questionnaires can help determine if there is a building-related problem. Demographics, health complaints, and location of respondents are acquired through this technique, which can also assist in the development of a sampling strategy, if necessary. The questionnaire may be standardized or tailored toward testing a particular hypothesis. Furthermore, the information collected may be compared to a database established by the Environmental Protection Agency (EPA) and the National Institute for Occupational Safety and Health (NIOSH). It is important, however, that respondents complete the questionnaire in confidence to maximize the accuracy of the responses (Macher 1999).

Sampling Strategy

If the visual inspection indicates that fungal growth or fungal indicators are present, then the potential for exposure may further be defined by utilizing various sampling techniques. For instance, air sampling may indicate that the spore concentrations in the air are related to the health symptoms being displayed by the building occupants or may assist in identifying hidden growth. Bulk or surface (dust) sampling may be used after visual observation to confirm. A good sampling strategy includes determining the materials to be sampled, sampling locations, the number of samples, and the efficiency of the appropriate sampling method and laboratory analysis. Sampling methods must be selected according to their ability to provide some measure or estimate of exposure. This typically results in the use of air sampling methods more so than others (Macher 1999).

Sampling Method

The traditional sampling method involves culturing organisms on nutrient agar. This method may be used for air, bulk, or surface sampling and is attractive because

of its ability to identify fungal species. Air sampling captures viable organisms on plates filled with agar via multi-hole impactors, whereas surface and bulk samples are washed and the resulting solute introduced to the agar. The agar is incubated for seven days at 25° C, after which a mycologist visually identifies and quantifies the fungal growth, if present.

Air sampling for spores (total propagule counts) involves the collection of spores on either a membrane filter or grease-coated slides. The filter or slide is then placed under a microscope to obtain the total fungal mass (viable and non-viable). Although some molds have distinctive spores, many, including those found indoors, do not. Thus, air sampling for spores may or may not be effective.

One type of air sampling technique is vacuum canister sampling, which is a technique that uses a vacuum canister to capture a known volume of air. The air is then analyzed via gas chromatography/mass spectrometry to identify any volatile organic compounds that may be produced by fungal activity. This method is attractive since some VOCs are indicators of specific fungal species.

Polymerase chain reaction (PCR) is a molecular biology method that is becoming more prominent for the identification of specific fungal species. It is more accurate than the above listed methods, but can only identify one species at a time. It is an effective identification method for both bulk and surface sampling (Macher 1999; Yang 2004).

Number and Location of Samples

The number of samples to collect depends on the objective of the collection process, the variability of the parameter being measured, the limitations of the sampling equipment, and labor availability. Based on these factors, the matrix at Appendix A may be employed for selecting the number of samples. Samples are typically collected from the areas in question, areas that are not considered to be problematic, and the outdoors. Outdoor samples should be collected upwind from the inlet closest to the problem area (Macher 1999).

Samples are typically collected from the areas in question, areas that are not considered to be problematic, and the outdoors.

The Dose-Response Relationship and Assessing the Risk

Culturable air sampling analysis results are reported in colony-forming units per cubic meter of air (CFU/m^3), and total propagule air sampling results are reported in spores per cubic meter (spores/m^3). There are no permissible exposure limits (PELs) or threshold limit values (TLVs) established by any regulatory agency in the United States against which to evaluate. Current opinion is that there is insufficient information available to establish a limit, although regulatory limits did exist in 1989 (United States Occupational Safety and Health Administration 2003; Macher 1999). Since no standard guidelines exist, the current common industry practice is to compare the concentration inside a building against the concentration outside the building, with lower concentrations indoors versus outdoors to establish the benchmark for "acceptable" concentrations. Also, indoor concentrations are to be compared to indoor concentrations from a non-affected area (Macher 1999; Yang 2004).

It is also recommended that the results be evaluated for rank order percentage (Macher 1999; US Micro-Solutions, Inc. 2005; Kemp et al. 2003; Spicer 2005). Indoor and outdoor concentrations may be similar in numeric value, but may contain different or varying amounts of fungi. For example, the total outside count from a building may be 2,500 spores/m^3 with 25 percent of the spores being ascospores and 75 percent being basidispores. The corresponding indoor count may be 1,500 spores/m^3, but 80 percent of the spores are *Aspergillus* and *Penicillium* and 20 percent are *Chaetomium*. This situation indicates that although the indoor versus outdoor concentrations are acceptable, the comparison of the types and percentage composition of the two samples implies that growth is occurring inside the building and requires further investigation.

There are also a few other types of sampling methods commonly used in industry practice today, some of which are regulated and some which are not. Bulk and surface sample analysis concentrations are typically reported in colony-forming units per unit area or per unit gram. As

with air sample results, there are currently no acceptable limits published by a regulatory agency in the United States. Vacuum canister sampling, on the other hand, does present the opportunity to compare analysis results against PELs or TLVs, with results being reported in parts per million (ppm) or milligrams per cubic meter of air (mg/m^3). PCR analysis is used in a different fashion in that it identifies just one species of mold. It is an investigative tool for confirming the presence of a target species.

Aside from the regulatory agencies, other groups or individuals have published guidelines for determining if a dose response relationship exists. Clark, for one, developed criteria for evaluation that was published in 2001. Normal background levels are detailed in Appendix B. The American Academy of Allergy, Asthma, and Immunology (AAAAI) developed a standard in 2002 based on how allergic individuals may react to spore exposure, using the scale detailed in Appendix C. It should be noted that these guidelines are based upon outdoor exposure. The World Health Organization, the Nordic Council, and the Russian Federation also published standards in 1988, 1991, and 1993, respectively, that recommended other sets of exposure levels (Rao et al. 1996; Brandys and Brandys 2004).

Discussion

Exposure to molds or fungi is unavoidable and occurs on a daily basis. Furthermore, outdoor molds are more abundant than indoor molds. Ten percent of the population is allergic to molds, with five percent expected to display any clinical illness. The most common allergic reactions are allergic asthma or allergic rhinitis (hay fever), with the most susceptible members of the population being the very young, the elderly, and pregnant women. Yet more importantly, the allergen concentrations that cause symptoms or sensitization are unknown.

Based upon information that has been presented though the media over the past 12 years, however, the general population is concerned only with overexposure to "toxic black mold." This is the result of the reports of the infant deaths reported at the Cleveland Clinic and the Ballard case, both of which revolve around the fungus *Stachybotrys chartarum*. The media failed to report that the original study concerning the infant deaths was withdrawn by the same organization that published the study report, the Centers for Disease Control and Prevention, following further investigation a few years after publication (Centers for Disease Control and Prevention 2000).

The media also failed to report that the Ballard case ultimately concerned an insurance claim by the Ballards against their insurance carrier for repair and remediation of their home from a series of water leaks, not a damage claim for health related effects. There are other celebrity cases (Erin Brockovich and Ed McMahon, to name a few) that have also been presented to illustrate the dangers of toxic black mold exposure (Trial Lawyers, Inc. 2006). Therefore, professionals are continually asked to determine if any suspected fungal growth is the toxic black mold and if the affected area is safe. Since there is currently no defined and recognized dose response information available, professionals must subjectively assess the risk to exposure.

For example, stained suspended ceiling tile, a common observable building condition, indicates a water intrusion incident occurred, but does not reflect future fungal growth or exposure. If a professional decides to take a sampling, he or she must determine which methods should be employed. Bulk sampling is the natural choice since it will provide a concentration of fungi present on the ceiling tile. However, many questions are raised by this method, such as whether or not the fungi are viable or dormant. If they are viable it must be determined if they are producing spores, and if so, whether or not those spores contain mycotoxins. A practitioner must delve deeper into the sampling to answer these questions.

Air sampling is typically performed to address these questions, but there is no one air sampling method that provides all the answers. A combination of total propagule sampling and culture sampling can determine the level of spore production and subsequent fungi growth (Macher 1999). Then the professional must select a guideline or guidelines against which to compare the sampling results. However, determining which one to use can be difficult.

The Occupational Safety and Health Administration and the American Conference of Governmental Industrial Hygienists at one time published exposure limit values for mold (Brandys and Brandys 2004). However, based upon the ongoing lack of dose-response information, both elected to withdraw these levels and concluded that indoor concentrations should be less than outdoor concentrations—the base standard that most professionals use today. It should be noted that even this position is problematic.

The AAAAI's 2002 standard, which defines outdoor exposure, states that a spore concentration less than 6,500 spores/m^3 is not considered to be an issue and no symptoms of exposure are anticipated. If one compares this to the "acceptable" concentrations in many of the indoor standards, one finds that the acceptable indoor levels are considerably lower. (This level ranges from 1,000 to 2,000 spores/m^3).

The laboratory analysis of samples is also a problem. Spore propagule and culture samples require a mycologist using a microscope to visually identify the fungi and then quantify them (Indoor Environmental Standards Organization 2002). *Aspergillus* and *Penicillium* fungi spores have the same appearance and are reported as an *Aspergillus/Pencillium* combined concentration. *Stachybotrys* spores are generally not identified in spore propagule samples because they do not become airborne easily and are found in a somewhat gelatinous material of the fungus. Not all fungi grow well on the same culture agar, so different agar must be used to identify many fungi. This is particularly true for *Stachybotrys,* which has difficulty competing with other fungi and is easily overgrown in common agars.

The number and location of air samples to collect is a major consideration (Macher 1999). Although many wish to know if they have the toxic black mold present and wish to identify its risk factors, even if they are at risk, many do not possess the financial resources required to have sampling performed at a rate that will provide data that is within the 95 percent confidence range. Costs for sampling at this rate could be in the tens of thousands of dollars.

As a result of all of these variables, a conservative approach is currently employed. If mold or fungi is present, exposure will occur, and an adverse health effect will develop. If air sampling is performed, samples are usually collected from the problem area, a non-problem area, and from outdoors. Results compare outdoors versus indoors, with rank order percentage of fungi identified (Macher 1999).

Conclusion

Complete freedom from any risk to mold exposure at the current time is not attainable. Thus, society must decide what risk it is willing to accept. Currently risk assessment is an extremely difficult task for a variety of reasons. The development of more accurate methods for sample analysis and collection are needed. In addition, the general population needs to be educated on the probability of exposure to molds and the subsequent heath related effects that may occur. Over the past decades, high-profile media reports on the effects of mold have brought much attention to the potential dangers of mold exposure. However, until a definitive dose-response relationship is established, quantitative risk assessment will continue to present problems for the investigative professional.

* *This reference was made in conjunction with a discussion on leprosy, which is caused by a bacterial infection, not a fungal infection.*

About the Author

George H. Bender, CIH, is the Manager of Environmental Health and Safety for Duquesne University in Pittsburgh. He is certified in comprehensive practice by the American Board of Industrial Hygiene and has more than 20 years of experience with occupational safety and health issues in schools and universities.

References

Brandys, Robert C., and Gail M. Brandys. *Worldwide Exposure Standards for Mold and Bacteria.* Hinsdale, IL: OEHCS, Inc., 2004.

Centers for Disease Control and Prevention. "Update: Pulmonary Hemorrhage/Hemosiderosis Among Infants–Cleveland, Ohio, 1993–1996." *MMWR* 49(09)(2000): 180–184.

Clark, Geoffrey A. "Assessment and Sampling Approaches for Indoor Microbiological Assessments." *The Synergist,* 2001.

Dearborn, Dorr G., et al. "Clinical Profile of 30 Infants with Acute Pulmonary Hemorrhage in Cleveland." *Pediatrics* 110 (2002): 627–637.

Dillon, H. Kenneth, J. David Miller, W. G. Sorenson, Jeroen Douwes, and Robert R. Jacobs. "Review Methods Applicable to the Assessment of Mold Exposure to Children." *Environmental Health Perspectives Supplements* 107(S3) (June 1999): 473–480.

DiNardi, Salvatore R. *The Occupational Environment–Its Evaluation and Control,* Fairfax, VA: AIHA Press, 1997.

Flappan, Susan M., Jay Portnoy, Patricia Jones, and Charles Barnes. "Infant Pulmonary Hemorrhage in a Suburban Home with Water Damage and Mold *(Stachybotrys atra)." Environmental Health Perspectives* 107(11) (November 1999): 927–930.

Hardin, B. D., B. J. Kelman, and A. Saxon. "Adverse Human Health Effects Associated with Molds in the Indoor Environment." *Journal of Occupational and Environmental Medicine* 45(5) (May 2003): 470–8.

Indoor Environmental Standards Organization. "Standards of Practice for the Assessment of Indoor Environmental Quality," Minneapolis, MN: IESO (April 2002).

Kelman, B. J., C. A. Robbins, L. J. Swenson, and B. D. Hardin. "Risk from Inhaled Mycotoxins in Indoor Office and Residential Environments." *International Journal of Toxicology* 23(1)(Jan–Feb 2004): 3–10.

Kemp, P. C., H. G. Neumeister-Kemp, B. Esposito, G. Lysek, and F. Murray. "Changes in Airborne Fungi from the Outdoors to Indoor Air: Large HVAC Systems in Non-problem Buildings in Two Different Climates." *American Industrial Hygiene Association Journal* 64 (March/April 2003): 269–275.

Macher, Janet. *Bioaerosols: Assessment and Control.* Cincinnati, OH: ACGIH, 1999.

Mann, Arnold. "Mold: A Health Alert." *USA Weekend* (December 5, 1999): 8–9.

Rao, Carol Y., Harriet A. Burge, and John C. S. Chang. "Review of Quantitative Standards and Guidelines for Fungi in Indoor Air." *Journal of the Air & Waste Management Association* 46 (September 1996): 899–908.

Robbins, Coreen, L. J. Swenson, M. L. Nealley, R. E. Gots, and B. J. Kelman. "Health Effects of Mycotoxins in Indoor Air: A Critical Review." *Applied Occupational and Environmental Hygiene* 15(10)(October 2000): 773–784.

Spicer, R., and H. Gangloff. "Establishing Site-Specific Reference Levels for Fungi in Outdoor Air for Building Evaluation." *Journal of Occupational and Environmental Hygiene* 2 (May 2005): 257–266.

Trial Lawyers, Inc. "A Parasitic Plague Spreads." 2003 (online); available from http://www.triallawyersinc.com/html/part07.html [accessed November 15, 2006].

United States Occupational Safety and Health Administration. "A Brief Guide to Mold in the Workplace." 2003 (online); available from http://www.osha.gov/dts/shib/shib101003.html [accessed September 3, 2004].

University of Georgia Plant Pathology Department. "Ergot: A History Changing Plant Disease." 2005 (online); available from http://www.plant.uga.edu/labrat/ergot.htm [accessed September 30, 2006].

US Micro-Solutions, Inc. *Micro-Notes,* Greensburg, PA: US Micro-Solutions, Inc. QA Department, June 2005.

Yang, Chin S. *Assessment of Fungal Contamination in Buildings.* 2004 (online); available from http://www.aerotechpk.com/Resources/TechnicalPaperDetails.aspx?i=54FFFC13-81FB-4C5F-AECC-9AF4748B4834 [accessed October 11, 2006].

Appendix A

SUGGESTED SAMPLE NUMBERS

Worst-case inhalation exposure	Monitor at least three worst-case exposure periods, and collect duplicate samples at each location
Average inhalation exposure	Monitor at least three times per day for three consecutive days, and collect duplicate samples at each location
Confidence interval around a mean exposure	Collect at least six samples
Variance of a data set	Collect at least 11 samples

Macher, Janet. *Bioaerosols: Assessment and Control.* Cincinnati, OH: ACGIH, 1999.

Appendix B

NUMERIC GUIDELINES FOR FUNGAL CONTAMINATION

Type of Sample	Normal Concentration
Air samples from residential buildings	<5,000 spores/m^3 <500 CFU/m^3
Air samples from commercial buildings	<2,500 spores/m^3 <250 CFU/m^3
Dust and bulk samples	<100,000 spores/gram <10,000 CFU/gram
Swab and tape samples	<10,000 CFU/in^2 <1,500 CFU/cm^2

Clark, Geoffrey A., "Assessment and Sampling Approaches for Indoor Microbiological Assessments." *The Synergist,* 2001.

Appendix C

AAAAI MOLD & POLLEN SPORE CONCENTRATIONS RANKING SCALE

Spore Concentration (Spores/m^3)	Ranking	Health Related Symptoms
None	Zero	No symptoms
>1 to 6,499	Low	Only individuals extremely sensitive to molds and pollens will experience symptoms
6,500 to 12,999	Moderate	Individuals sensitive to pollens and molds will experience symptoms
13,000 to 49,999	High	Most individuals with any sensitivity to pollens and molds will experience symptoms
>50,000	Very High	Almost all individuals with any sensitivity to pollens and molds will experience symptoms

Brandys, Robert C., and Gail M. Brandys. *Worldwide Exposure Standards for Mold and Bacteria.* Hinsdale, IL: OEHCS, Inc., 2004.

Proverbial wisdom counsels against risk and change.

But sitting ducks fare worst of all.

—Mason Cooley (1927–2002), American aphorist

Assessing RMIS Needs for Colleges and Universities

David A. Tweedy, CMC, Practice Leader for Risk Information Consulting Practice, Albert Risk Management Consultants, Inc.

Abstract: What is an RMIS, and why is it important for collegiate risk managers? While many if not all already have risk management information systems (RMIS) in place, some may not be aware of how to assess the effectiveness of their existing RMIS, or the feasibility of upgrading to a more efficient system if necessary. This article offers strategies for conceptualizing an RMIS system customized to the individual risk manager's needs in his or her specific context.

Introduction

Improved efficiency. Lower cost of risk. Ongoing performance measurements. Elimination of repetitive, manual tasks. Increased ability to spot disturbing risk trends. Increased visibility to senior management.

Sound good? They should. Most vendors providing commercial, off-the-shelf risk management information systems (RMIS) have been claiming those results for years. And there are more than 50 systems, plus or minus 10 percent, which offer a wide variety of commercial solutions for all types of industries.

But in spite of success stories across many industries and with various client sizes, there have also been complaints such as: "the RMIS is too claims-focused"; "it doesn't really deal with my specific problems or industry"; and, the clincher, "it's too expensive."

As a result, there seem to be fewer comprehensive, commercial RMIS systems used by colleges and universities. Instead, most collegiate risk managers use a hodgepodge of software and manual activities that can be generically referred to as their own RMIS. Microsoft Office (with Word, Excel, PowerPoint, Access and Outlook) seems to be the software of choice because of its many functional uses, relative user-friendliness, and widespread acceptance and use across many industries.

Most collegiate risk managers use a hodgepodge of software and manual activities that can be generically referred to as their own RMIS.

But do these homegrown systems really generate the types of results that commercial system vendors promise? Certainly they are inexpensive, but do they yield sufficient and tangible results?

Objective

The purpose of this article is to explore the value of risk management information systems for colleges and universities. It will define an RMIS, evaluate its usage and significance, discuss leading commercial vendors, address enterprise risk-related tools, and more.

Is the Collegiate Risk Management Environment Unique?

While all risk management positions have a common base, there are certain nuances in the collegiate environment that should influence the type of RMIS implemented. Some characteristics are:

- ***Non-claim based:*** RMIS came into existence in the 1970s due to clients with high volumes of claims (mostly Workers' Compensation and liability) who desired a better way of analyzing them and their causes. It is not that universities do not have these losses; they are, however, less claims intensive in frequency. Most colleges and universities are exposure driven.
- ***Exposure driven:*** Colleges and universities have a wide and diverse set of exposures that need tracking and analysis. These include (but are not limited to) study abroad programs, external community events at college facilities, medical centers/teaching hospitals, construction projects, terrorism risks, club sports, pollution liability, release of toxic elements from laboratories, fine arts, etc. And they also have claims. The chosen RMIS must reflect these exposures.
- ***Lean staff:*** Many universities and colleges have small risk management departments. The risk manager

wears many hats and must depend on the resources and services available.

- ***Budget limitations***: While this seems to be endemic in all of risk management, it is especially true here. Risk managers have to make more of less.

What, therefore, would a collegiate RMIS look like? What elements should it contain?

Here are some characteristics:

- ***Cost-effective:*** The system should be inexpensive enough that a quick payback can be shown through its use.
- ***Easy to learn and use:*** Most risk managers are not "techies." The system should be intuitive and easy to appropriate. This also applies to the attached report writer (including graphics).
- ***Adaptable/flexible:*** The system should be able to incorporate claims, exposure, and financial analysis with a demonstrated ability to be used across a wide spectrum of activities. It should be easy to alter without affecting the underlying code.
- ***Inclusive:*** The system should be able to use or access collaborative web-based tools (Web 2.0) such as eRoom or SharePoint (or similar).

Many traditional RMIS do possess many of these qualities. It can be easier if the risk manager can use an off-the-shelf package rather than creating one.

With this foundation, what does the commercial RMIS industry look like today?

FIGURE 1
THREATS RISK MANAGERS FACE

Macro Threats	Micro Threats
Increased compliance pressures	Information flow bottlenecks and gaps
Constantly changing system technologies	Integration issues
Limited resources to spend on RMIS improvements	Disparate data sources, data accuracy issues
Increased globalization	Vendor support issues
Shrinking risk management department staff	Limited internal IT availability

The RMIS Landscape

The risk landscape has changed with the advent of Sarbanes-Oxley, the Patriot Act, and recent acts of terrorism. Even privately held or non-profit organizations feel the impact. Figure 1 summarizes just some of the risks that a risk manager faces today.

More than ever, risk managers need a well-designed risk management information system. This is a computerized composition of software applications and databases that enable risk managers to evaluate information and make informed decisions. It should, ideally, mirror the risk management process: gathering data, analyzing/synthesizing, decision-making on risk financing and risk control issues, and reporting those findings and results.

More than ever, risk managers need a well-designed risk management information system.

The RMIS must be powerful, yet easy to use. It must be capable of providing a big picture view of diverse data, but also be able to provide detailed analysis on specific data. The data on which the RMIS relies must be accurate and thorough. The RMIS must be able to effectively interface with other key systems within the organization, and to keep up with technological advances without being too focused on needless "bells and whistles." Above all, the RMIS must be cost-effective and capable of handling the new challenges that the increasingly beleaguered risk manager throws at it.

How is this possible for a risk management department that has less time to worry about managing technical problems? Moreover, how can the risk manager function in today's dynamic business environment and not use well-designed and efficient technology? It is truly a Gordian knot.

Consider the following two-phase process. The first phase centers on following a logical process to determine and prioritize needs before taking action.

Phase 1: Assessing Your Needs

You Already Have a System

When the term RMIS is used, most risk managers think of commercially developed and sold solutions, such as those from CS Stars, Aon, or CSC.

Some risk managers think that they have no need for an RMIS and never will. But interestingly enough, all risk managers have some type of information system. Consider one of the baseline definitions of "system" from *Webster's Dictionary*: "A group of interdependent items that interact regularly to perform a task."

Regardless of the format or where it is stored, all risk managers have policies, claims, exposure lists, auto schedules, certificates, and contracts. There is also an established set of business procedures that govern how data is gathered, analyzed, organized into some type of report, and submitted. That is a system by any definition. The key questions are: How efficient is that system in identifying, analyzing, and managing the risks of the organization? What tools are being used to help the risk manager in this effort? What are the barriers facing this effort?

Today, risk managers are expanding their activities into enterprise risk management (ERM). ERM involves even more data, processes, and systems. Indeed, as will be seen later, the number of ERM systems is far more than the traditional RMIS.

Yes, everyone has a system. And if so, they also have the problems that correlate with systems.

Everyone has a system. And if so, they also have the problems that correlate with systems.

Traditional Problems and Barriers

Today's increasingly complicated IT and risk landscapes generate many challenges. Some of them have already been listed. To properly assess RMIS needs, a clear understanding of the problems and barriers is necessary. These issues can be divided into two separate areas of traditional risks and enterprise risks, as defined by the report issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Traditional risks are those that risk managers have dealt with for decades: risk of fortuitous loss to property and human resources. Traditionally, an RMIS receives, consolidates, and analyzes data; generates reports; tracks exposures; and performs various administrative duties (policy tracking, asset tracking, etc.). The following are issues relating to these RMIS:

- ***Multiple data sources/data accuracy:*** Many companies and organizations have multiple lines of coverage, complicated by multiple insurers and third-party administrators (TPAs) over the years. That means a lot of data that must be tracked. The problem is that the electronic data is rarely stored in similar ways among the various providers. For example, the details of a back claim are recorded by insurer A in a different manner than insurer B. Consolidating this data into one unified source takes time and effort. Further complicating this situation is that data errors typically abound, either in recording the information, or in transferring it to another media or provider. Oftentimes, this is the single most difficult issue facing a risk manager in assessing true RMIS needs. It is like an iceberg—most of the problem is below the surface.
- ***Complex and diverse reporting needs:*** The primary output of any RMIS is reports. The report-writing tool must be easy to use, yet able to perform complicated analysis. The reports must be quickly available and provide a good overview with graphical representation if need be. The tool should also provide good "drill-down" capability and provide the backup details of an analysis. Unfortunately, many systems today are challenged in this area. The tool is either too user-friendly and unable to provide the detailed analysis, or it is very powerful and too difficult to use.
- ***Increased demand for faster, deeper analysis:*** The advanced RMIS must operate as a business intelligence tool. Drawing data from diverse sources, organizing it, and presenting it quickly and flexibly to risk managers is a necessity. Unfortunately, many risk managers must spend hours entering data and preparing the reports to run, sacrificing analysis time to time-consuming manual activities. This is both counterintuitive and nonproductive.
- ***Vendor support:*** An endemic problem in the IT and insurance industries is the level of support provided by the vendors to their clients. It is no different in the RMIS sub-industry. Off-the-shelf software applications have great advantages. However, the

drawback is that some customization is necessary, and constant data conversion issues may occur. Bugs, viruses, downtime, faulty reports, and interface issues with internal accounting systems all require proper vendor support. Yet, the vendors themselves have resource limitations, too. How do they properly allocate them among their customer bases?

- ***Limited IT resources:*** Vendors are not the only ones facing resource scarcity issues. Internal IT departments, especially since the advent of various federal legislation (such as Sarbanes-Oxley, the Patriot Act, the Health Insurance Portability and Accountability Act, and the like) are under constant pressure and scrutiny by senior management. Risk management departments are typically not high up on the IT priority list.
- ***Integration issues:*** Integrating RMIS with internal systems—such as the general ledger, payroll, and human resource systems—represents both opportunities and problems. RMIS vendors will tout the ease of plugging their system into the milieu of a corporation's internal IT structure. However, while system technology, through service-oriented architecture (SOA), is moving toward an easier integration environment, this is still not widespread enough. Potential problems abound, which necessitate thoughtful planning before opportunities can be realized.
- ***Technology obsolescence:*** None of these issues exist in a vacuum—many vendors and customers alike suffer from technology obsolescence, and that has a decided impact on the type of systems in which one can invest. Yet the problem in not dealing with the obsolescence has profound effects, too. Web-based solutions through application service providers (ASPs) help the risk manager to avoid internal architecture limitations, to be sure, and many vendors now offer this type of system.
- ***Cost:*** It is common for the cost of the system to be a major focus of risk managers. What is the annual license fee? What about the annual service fee? What is the cost to customize a module? Or build an interface? What about the cost of converting the data to the new system's format? These and others are good questions. But it must be recognized that there is a cost in doing nothing, too. In fact, the cost of doing nothing may have a larger economic impact on the organization. These are the questions that risk managers must answer to make an informed decision.

COSO defined enterprise risk management (ERM) as a process initiated by senior management defining and quantifying risk in the context of an organization's vision, mission, and business strategies. Accordingly, these issues involve expanded areas of risk, such as business risk, speculative risk (hedge funds), market risk, and governmental/compliance risk. When an ERM initiative is undertaken, the RMIS/IT issues expand accordingly.

The cost of doing nothing may have a larger economic impact on the organization.

- ***Compliance:*** Sarbanes-Oxley (SOx), the Health Insurance Portability and Accountability Act (HIPAA), and similar federal and state acts require a careful monitoring and documentation of business processes, such as disclosure procedures for employee information and other important activities. To be truly helpful, good information on these business processes (i.e., where the gaps and bottlenecks are) must be immediately and accurately transmitted to executive officers. Accordingly, systems must be able to handle this.
- ***IT security:*** There is the ever-present, and growing, threat from hackers who seek to either damage IT structures or get access to valuable client, employee, and financial data.
- ***Business processes monitoring:*** ERM practices are more developed in financial industries, such as banks and insurance companies with high volumes of transactions and well-defined processes. Adoption and embedding of ERM practices within organizations with less defined business processes are not as frequent. Many IT firms are marketing business process monitoring (BPM) software applications to help clients analyze and modify business processes to comply with ERM objectives. BPM systems, in effect, can be regarded as a type of enterprise risk

management information system (ERMIS) as they are tools that help satisfy ERM goals.

In the end, ERM is dependent on the availability, accuracy, and timeliness of information reaching senior level management to equip managers to make proper decisions. Sound familiar? It is the same objective that the risk manager has in using a traditional RMIS.

Not all risk managers will face each of these issues, but they will experience enough to identify some clear needs in their current RMIS configuration. This is where risk managers must determine their own prioritized lists of needs and the level of detail that is necessary to deal with those needs. While risk managers should intrinsically know the state of their programs, it is wise to go through a defined process.

Conduct Issues Review

Step one is an honest appraisal of the RMIS issues within the organization. Is there a technology gap? (Is the organization still using client/server technology? Windows 95?) How many data sources exist? Is there a need for consolidation into one source? Is the data really accurate? Are you comfortable with the level and accuracy of the reporting? Are costs properly and easily allocated among divisions or is there painstaking maintenance of an ever-expanding Excel spreadsheet? Are compliance issues within your scope of activities? Does the organization frequently reorganize? Do mergers and acquisitions occur often? Are there complex risk financing programs in place? Are there foreign operations? And the most important question: Does the current RMIS satisfy the demands placed on it?

FIGURE 2
INDICATORS OF A NEED FOR AN RMIS

Multiple data sources (more than three)	Large volume of historical claims data
Small internal risk management staff	High frequency of mergers/ acquisitions
High frequency of WC and/or GL claims	Complex hierarchy, constantly changing
High Sarbanes-Oxley exposure	Complex internal charge-back procedures
Complex insurance program	Small and/or unresponsive IT department
International exposures	Self-administered claims program
Complex and/or diverse reports	Frequent vendor changes (broker, insurer)

Consider the table in Figure 2 showing indicators of the need for a comprehensive RMIS solution. If an organization has three or more of these situations, a solid RMIS is essential.

Similarly, Figure 3 provides a simple activities-based test to help perform an assessment. A "yes" answer to three or more questions means the current RMIS is in need of adjustment, or at least some thoughtful scrutiny.

FIGURE 3
RMIS SELF-ANALYSIS TEST

Question	Y/N
Do you spend more than 10 hours a week on repetitive, manual tasks (e.g., data entry, copy and paste type reports)?	
Do you have more than three separate sources of claims data?	
Do you spend more than four hours making sure that the data is properly consolidated and accurate?	
Do you spend more than one hour requesting a report from your RMIS?	
Do you spend more than two hours adjusting your RMIS when your company reorganizes its hierarchy or acquires a new company?	
Does it take longer than four hours for your RMIS vendor to respond to service inquiries?	
Do you need to access two or more systems to reach a final significant decision?	
Do you manually maintain certificate of insurance lists and/or exposure lists (properties, autos, etc.)?	
Are you frequently ignored by your internal IT department on critical issues?	
Does your RMIS negatively affect (either in time or substance) your decision-making process?	

Determine Scope

Step two is to determine the scope of the system needs assessment. There are three options.

1. ***Do nothing:*** This is a necessary option to consider and one that many unconsciously choose when confronted with this type of analysis. Yet recognize that it is also an active decision to "do nothing." It means that you are able to adequately confront the issues listed above with the tools at hand.
2. ***Tweak:*** If after evaluating step one, the risk manager determines that the needs are *mostly* met by the amalgam of internal systems, external systems (from an insurer or TPA or broker), and/or existing off-the-shelf RMIS, then minor modifications are in order. For the purpose of the rest of

FIGURE 4
TOP RMIS VENDORS—SYSTEMS AND CONTACTS

Bundled RMIS Providers

AIG—Intellirisk
Director Alan Louison
alouison@aig.com

CNA—Clearview
Director Nancy Giecewitz
nancy_gicewitz@cna.com

Cambridge Integrated Services—Claims/Reporting System
Senior Vice President Tracy Mock
tracy.mock@cambridge-na.com

Chubb—RMIS Dimensions, Loss History Analyzer, ClaimView
Richard Kaiser
rkaiser@chubb.com
(800) 715–7475

ESIS/ACE—RiskAdvantage
Frankie Santos-Ragin
frankie.santos@esis.com
(215) 640–1855

Frank Gates, Inc.—G2 WebLink Gates2000
general@frankgates.com
(800) 777–4283

GAB Robins—EyeAdvisor
Andrew Miller
millerba@gabrobins.com
(973) 993–3524

Gallagher Bassett—RisxFax
Colleen Saurbier
colleen_saurbier@gbtpa.com

Hartford/SRS—@venture
Cathy Leonard
cathy.leonard@thehartford.com

Liberty Mutual—RiskTrack
Alicia Rawnsley
alicia.rawnsley@libertymutual.com

Sedgwick CMS, Inc.—Juris
sedgwick_cms@sedgwickcms.com
(901) 415–7400

St Paul Travelers—eCarma
Vice President, RMIS,
Matthew Cardin
matthew.l.cardin@stpaultravelers.com

Zurich of North America—RiskIntelligence
(877) 263–0583

Unbundled RMIS Providers

American Technical Services—ATS/RMIS
Nick Zivlovich
nickz@atssales.com

Aon— RiskConsole
Kathy Burns
kathleen_m_burns@aon.com

Blackburn—RiskPro
sales@blackburngroup.com

Brightwork—Alyce Claims Management System
Ted Lukens
tedlukens@brightworkinc.com

CSC—RiskMaster
Sales: (800) 345–7672

CSStars—STARS
Jeffrey Markowitz
jmarkowitz@csstars.com

DAVID—Renaissance, NavRisk
Mary-Margaret Dale
mdale@davidcorp.com

Delphi Technologies—Oasis
Peggy Randolph
prandolph@delphi-tech.com

Effisoft—Webrisk
Will Warren
will@effisoft.com

Emerson Software—eRMIS2
Sales: (910) 794–1616

Envision—RiskEnvision
Scott Harper
sharper@envision-ts.com

Exigis, LLC—WorkFlow Solutions
Armand Alvarez
(800) 928–1963

GenSource—GenIris, GenComp, GenPac, GenDis
Michael Kosten
(800) 949–9192

INFORM Applications—Inform RMIS, Inform Claims
Steve Sheridan
steve_sheridan@ibi.com

JW Software—Filehandler
Tim Cuckow
(440) 519–1740

Occusoft—RiskPro
sales@occusoft.com

OCI—RMIS
Steve Tomsic, Sales
steve_tomsic@oci.com

PerDatum—Prognos
Sales: (800) 351–1370

Risk Sciences Group—Sigma Encore
Manny Quintana
manny.quintana@risksciencesgroup.com

Valley Oak—VOS
Randy Wheeler
rwheeler@valleyoak.com

Visual Risk Solutions—Visual Risk Portal
info@visualrisksolutions.com

WLT Software Enterprises—WLT RMIS
info@wltsoftware.com

Sources: Business Insurance's annual directory of RMIS; RMISWeb's listing (www.rmisweb.com); and Risk and Insurance's annual directory.

this analysis, it would be useful to follow the next option template (overhaul) and co-opt whatever is necessary to achieve a desirable end solution.

3. ***Overhaul:*** This option means that the current situation is clearly detrimental to the risk manager getting the job done. It can also be further subdivided into either a build, buy, or hybrid approach. And it is important to really evaluate what kind of solution is needed.

Conduct a Preliminary Review of Potential Solutions

Assuming a decision is made to obtain a new RMIS (overhaul), the next step in the process is to determine whether it will be an off-the-shelf solution through the available commercial vendors in the marketplace. At present, there are more than 50 traditional RMIS vendors and about two to three times that number of ERMIS vendors. Figure 4 lists most of the top RMIS vendors, governed chiefly by numbers of clients and users.

The capabilities and approaches are significantly different. Some risk managers actually access several RMIS providers, depending on their program makeup, especially if they have multiple insurers, brokers, and TPAs involved.

Designing or selecting the best RMIS, whether it is a stand-alone application or an amalgam of different systems, first requires a survey of available systems. Lists of many of the vendors are published periodically in *Business Insurance* and *Risk and Insurance* magazines, and a list is included on the RMIS website (www.rmisweb.com). Soon a comprehensive review of these systems will also be available from the Institutional Risk Management Institute (IRMI).

The best method to categorize RMIS vendors is by looking at several critical factors: ownership, portability, business intent, system functionality and configuration, and price.

- ***Ownership:*** Most RMIS vendors are owned by some type of insurance service provider (insurer, broker, TPA, or medical bill reviewer). However, a good number are either independent or are funded by equity capital firms. Still others are owned by large system integrators. Ownership suggests the type of investment placed in the system, the target market pursued, and the resources available for research and development. How long have the vendors been providing RMIS?

- ***Portability:*** The next differentiator is focused on the systems provided by these vendors. Most provider-owned systems are not portable, or unbundled. That means the system only stays with the client as long as the client stays with the vendor. This is a significant issue, especially if you've been with one of these bundled systems for a long time.
- ***Business intent:*** This is very important. What are the primary, secondary, and even tertiary business intents of these RMIS vendors? Is it claims management (tracking), claims administration (claims management plus check-cutting), risk analysis, policy administration, or some or all of the above? What are their strengths and weaknesses? For example, it stands to reason that most insurer-owned RMIS are focused on the products/services they provide, such as claims administration, safety/loss prevention, and policy information, while independent systems typically provide a more comprehensive approach. It depends on the risk manager's primary needs. One shouldn't purchase a sledgehammer when only a tack hammer is required. Further, what target markets does the RMIS vendor pursue? It would make sense to pursue vendors with a specialty focus on your industry, be it healthcare, banking, maritime, etc.
- ***System Functionality:*** This is more of a drill-down into specifics. What lines of coverage does the RMIS handle? What kind of reporting tool does it have? How well does the vendor handle knotty issues like data conversion and integration?
- ***System Configuration:*** What types of system solutions are offered? Client/server or web-based? Is there a leasing or site license option? Are time-share solutions offered? What are the applications written in? Who are the system business partners (e.g., Oracle and Microsoft)?
- ***Price:*** This is a very difficult variable to compare on an "apples-to-apples" basis. A useful comparison tool would be to ask the vendors what type of pricing they would offer under certain business scenarios. For example, provide several vendors with a profile indicating the number of claims, data sources, locations, lines of coverage, and types of reports needed. Then ask for an indication of the estimated cost and the ongoing service cost (it is usually a percentage of the first year license fee). In a formal RMIS bid project, details of the pricing will be more explicit. The objective here is to get a preliminary read on the potential cost.

Phase 2: Designing the Solution

A SWOT analysis provides a means for reviewing how well the current system and business procedures work or do not work.

At this point, the all-important first phase of preliminary RMIS assessment by the risk manager is completed. Although nothing formal has been done, it is very important that those steps be completed to really evaluate the state of the current system(s) that are being used. Now that the real issues and challenges are identified, it is time to determine what type of systems should be pre-selected for potential consideration.

That decision may or may not involve non-traditional software solutions. For example, it may be that a better use of Microsoft Office and some collaborative web tools such eRoom or SharePoint is more in line with the ultimate goal.

Indeed, because collegiate environments are typically not claims oriented (as was discussed earlier), a RMIS solution may not involve a traditional off-the-shelf application.

This second phase is all about design, selection, and implementation. The assumption going forward, as in the first phase, is that a total overhaul is required. The following steps offer one possible template for proceeding.

Begin SWOT Analysis. After going through phase one, performing a SWOT analysis (strengths, weaknesses, opportunities, and threats) is an excellent way to begin phase two. A new system should not be conformed to the existing business practices until they, themselves, are vetted. A SWOT analysis provides a means for reviewing how well

the current system and business procedures work or do not work. Back in the beginning of the first phase (acknowledging that you already have a "system"), the risk manager, in essence, began this SWOT assessment. Strengths and weaknesses should be very obvious at this juncture. Threats and opportunities, however, might not be.

To identify threats, a good question to ask is, *If I do nothing, what will happen?* To identify opportunities, a good question to ask is, *If I implement a new system, what benefits will likely occur?* This is an excellent segue into the second step—conducting a cost/benefit analysis.

Conduct Cost/Benefit Analysis. To secure the time and resources needed to either implement a new RMIS or significantly adjust an older one, a cost/benefit analysis is critical. The SWOT review, combined with some preliminary information gathered on potential vendor solutions, should qualitatively identify the benefits and costs associated with a new system.

Quantifying the expenses is easy: software license fees, hardware, ongoing service, conversion costs, custom programming, telecommunication expenses, etc. Quantifying the benefits, however, is more difficult because many of them are so-called "soft benefits." These benefits will be different for each organization due to its unique circumstances. For example, through comprehensive policy administration module, an RMIS identified double coverage for business interruption when comparing a global program with a domestic one, and eliminating the duplicate policy saved $80,000 in premium. Improved claims-monitoring software identified $200,000 in duplicate payments or inaccurate reserves for this same company. Through use of a reasonable return on investment equation, the risk manager was able to identify a payback period for the investment of only 18 months.

Obtain Senior Management Approval

Completion of the first two steps provide the information needed to obtain approval for the project. Showing a positive return on investment (ROI) and a well-thought-out SWOT analysis often earns a quick approval from senior management. This would be especially true if managers themselves are under scrutiny for implementing enterprise risk management practices in all of their business operations. It may even provide an opportunity for the risk manager to gain additional authority to work with senior management on ERM initiatives.

Establish RMIS Search Committee

Armed with senior management approval, the risk manager now has the authority to organize the search committee. It is important for the risk manager to identify those in the organization critical to the success of a comprehensive RMIS. Who are those stakeholders that stand to benefit or profit most from a new system? Also, who have

FIGURE 5
EXAMPLE VENDOR RATING MATRIX

Issue Evaluated	Rate 1 (low) to 5 (high)	Priority 1 (not critical) to 3 (critical)	Total Score = Rate x Priority
General Questions			
How well did the proposal meet RFP requirements?	5	3	15
How clear was the vendor's presentation?	4	3	12
What is the length of time in business (stability)?	5	2	10
What is the number of implementations (experience)?	4	2	8
What is the financial strength?	5	2	10
Will vendor allow "test drive" before final contract acceptance?	1	1	1
			Average 9.33
Overall System Functionality			
Integrated database of Excel spreadsheets data, including claims	5	3	15
Real time data entry	5	3	15
Automatic updating of database once changes to claims, financial transactions or policies are made	5	3	15
Simplified data entry; error reduction built in, eliminate redundant entry	5	3	15
System security (levels of access)	5	3	15
Authority levels for payments, reserve changes, etc.	5	3	15
Flexible hierarchy management	5	3	15
Internal intranet Access	5	1	5
			Average 12.00

been the most vocal critics? Sometimes, it is wise to have those critics involved in the process to build understanding and consensus.

Moreover, it is also very important for someone from IT to be part of the committee to ensure that internal standards are met. Having someone from IT well acquainted with the RMIS will only benefit the system, especially if it is to be integrated with other internal systems.

Formalize the Needs Assessment

The risk management department is really an information clearinghouse: data flows in, is collected and analyzed, and then information flows back out in the form of reports. Thus, the next step is for the RMIS committee to divide up the organization in a logical fashion and identify the needs of other departments and individuals by querying them. Of ultimate importance is what senior management desires. This will grow in intensity and urgency as enterprise risk issues begin flowing through the risk management department. Now the SWOT analysis is complete.

Identify/Prioritize Options

Needs must be ranked by importance of meeting them as well as by the difficulty of satisfying them. For example, there may be a highly defined need to put together a comprehensive cost-of-risk allocation module, but the anticipated customized programming involved might end up being cost prohibitive when compared to the benefit derived. The results of this process will yield system specifications for the upcoming bid project.

Needs must be ranked by importance of meeting them as well as by the difficulty of satisfying them.

Select RMIS Vendors To Approach

Using the information about potential systems that was developed in phase one, three to five potential RMIS providers that best meet the requirements list should be selected. It is unwise to consider more than five vendors because the bid process becomes unwieldy.

Compile Specifications/Request for Proposal (RFP)

System and user specifications are detailed in this document along with whatever formal RFP guidelines the organization prefers. Typically, the IT manager on the RMIS committee or a procurement agent will be the point-person at this stage.

Conduct Bid Project

Once the RFP/specifications package has been released, it is typical to allow between 30 to 60 days for responses, depending on the size of the system and number of vendors involved. It is customary to allow a question-and-answer meeting (which can be handled via web conference instead of on-site) to clarify potential misunderstandings. Some projects also allow on-site or web conference demonstrations to the RMIS committee to further clarify differences between the participating vendors and systems.

The ultimate selection is performed by the committee after a careful examination of the proposals, interviews, and presentations. It is helpful to use a vendor-rating questionnaire that seeks to eliminate subjective decision-making and encourages a quantified rating by the reviewer. Figure 5 provides an example. The needs are listed in the left column, a weight is given to the attribute (typically between 1 to 3), and a rating (typically between 1 to 5) is assigned. The weight is multiplied by the rating for a score on that attribute. The total score is then added and compiled with other reviewers to help reach a final conclusion.

Once the system and vendor are selected, the next step is one that is frequently overlooked, but is extremely critical.

Do Not Forget Implementation

Two of the most overlooked, yet crucial, issues regarding RMIS are data management and system implementation. Data problems were mentioned in phase one. Implementation is the all-important "danger below the surface" issue in phase two. Those risk managers who give it short shrift do so at their peril.

From the signing of the contract to screen and report design, rollout of the application, interface construction, data conversion, parallel testing, and turnover to the new system, there are many places where breakdowns can

occur. That is why the RMIS committee needs to stay together until the system is actually deployed. Sound project management techniques should be followed by setting clear timelines with linked dependencies, due dates, and regular updates to the plan. Meetings with the vendor should take place weekly to make sure that the tasks and deadlines are being properly assigned and met. The contract itself should contain penalty clauses if the project is delayed because of the vendor. Similarly, it is good to build in incentives to reward an installation of the system ahead of schedule.

Constant Monitoring

Another good practice is to keep the RMIS committee together during the first year to monitor the progress of the new system. A goal should be to document improvements in processes and savings from the presence of the RMIS. Because the RMIS touches on most parts of the organization, the risk manager has an excellent opportunity to strengthen ties with other departments while providing valuable information horizontally and vertically to senior management.

A Potential Solution Scenario: (A Possible Case Study)

For argument's sake, let us assume that the risk manager has performed the above needs assessment procedures and has determined that a hybrid approach is warranted. He or she has a pre-existing relationship with a broker that has a bundled system that takes claim feeds and provides online access to the risk manager. The budget is extremely limited and too small to afford a full-blown unbundled RMIS solution. The risk manager has Microsoft Office (Word, Excel, PowerPoint, and Access) and uses Outlook for e-mail.

What could the risk manager do?

- ***Set priorities/establish a plan:*** The needs assessment process will help do this for the risk manager. Priorities will be established.
- ***Leverage all technology opportunities:*** MS Office is probably the most popular RMIS today, although it is not typically called one. Many risk managers plan their budget and keep schedules of autos, properties, and policies on Excel, and put together presentations with PowerPoint. More advanced risk managers will use Access for claims databases. But other generic software can be used. SharePoint is a low-cost collaborative software tool that can be used for the all important communication application that would keep the risk manager in touch with key people inside the university and vendors and contacts outside the university. This may be the most important part of the collegiate RMIS: getting the risk manager's contact list on the collaborative shareware application.

  There are also some low-cost, powerful applications for creating risk maps, and other such quantitative software.
- ***Invest dollars in most significant area:*** Only the results of the needs assessment will show what this is. Many may choose to fortify their risk management website, making it more informative, interactive, and rich with information, from risk management procedures to how to file a claim. This can be a separate topic in itself.

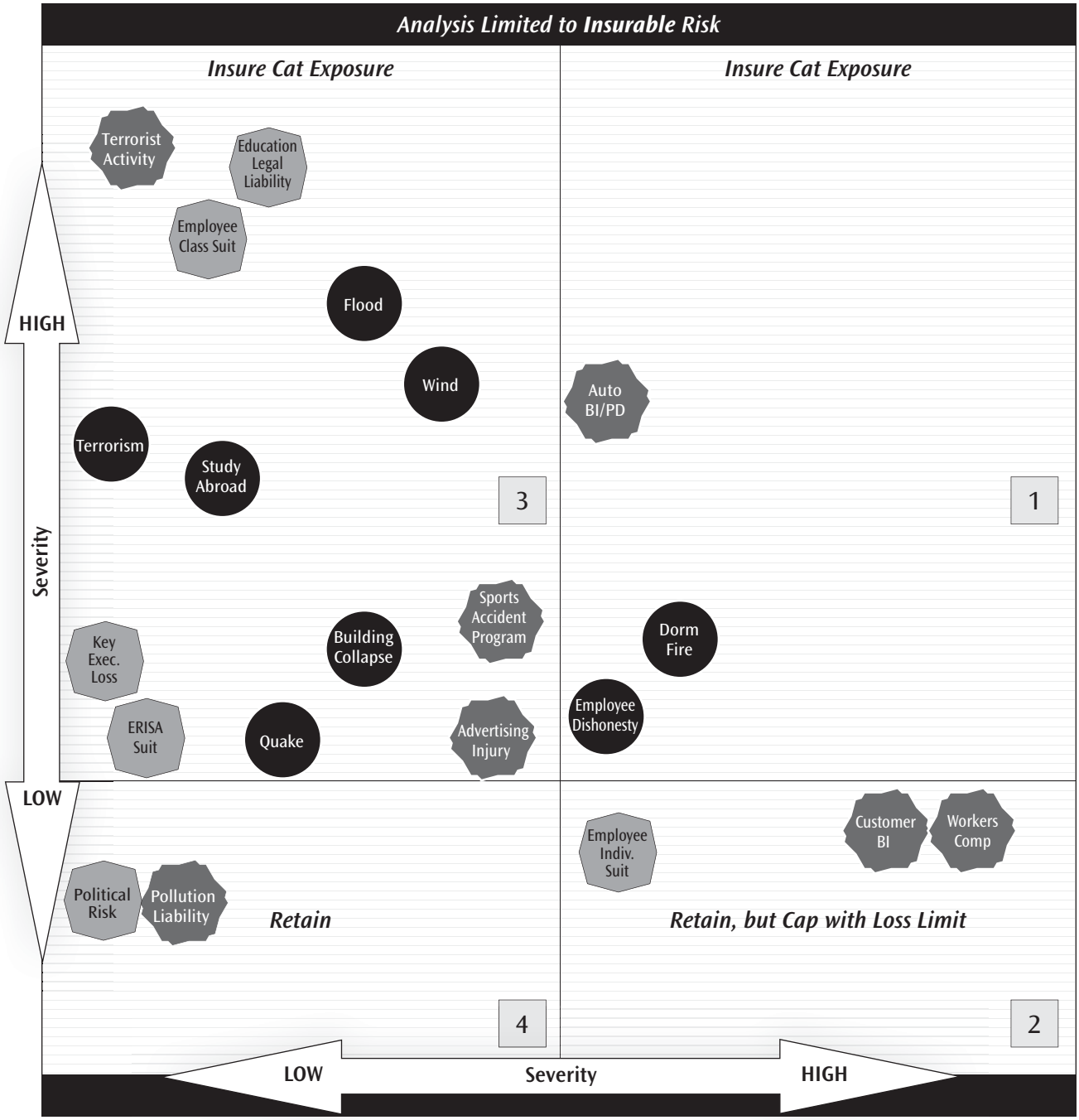
Conclusion

Going through a detailed RMIS needs assessment and selection/implementation process may be a painful experience. However, the knowledge, experience, and benefits derived from a well-executed process will yield significant benefits to the risk manager and the organization alike.

About the Author

David A. Tweedy, CMC, is the RMIS Solutions Practice Director of Albert Risk Management Consultants' (ARMC) Risk Management Information Systems practice. He provides clients with risk information technology advice and services, is an internationally recognized expert in the RMIS and claims management arena, and has more than 24 years of experience as a risk management consultant. He holds a B.S. from the University of Massachusetts in Amherst, and an M.B.A. from the University of Rhode Island in Kingston. He is also the author of *RMIS Review,* which was published by IRMI in 2007. Mr. Tweedy can be reached at DTweedy@albertrisk.com.

University/Collegiate Risk Map (Sample)



I think one's feelings waste themselves in words; they ought all to be distilled into actions which bring results.

—Florence Nightingale (1820–1910)

In Case of Emergency: Selecting a Qualified Air Ambulance Provider

Denise Treadwell, CRNP, MSN, CEN, CFRN, CMTE, Executive Vice President, AirMed International

Abstract: When emergency injury or illness necessitates air medical evacuations, it is important to have a reliable air ambulance provider. Such transports may often involve extended times outside of a medical facility, especially during international flights. This article provides an overview of requirements air ambulance providers must meet, as well as other safety measures that must be considered to ensure the well-being of patients, flight and medical crew, and passengers during transport.

According to studies conducted by the Centers for Disease Control (CDC), more than 65 million U.S. residents travel abroad each year. Relatively few of these travelers are prepared for a medical emergency, yet the risk for illness or injury remains high in all travel situations. One of the most common causes of injury during international travel is motor vehicle accidents, for which few are prepared. And illnesses that affect travelers include cardiovascular complications, infectious diseases, respiratory illnesses, and other medical related diagnoses. Preparing for these and other adverse circumstances has never been more important than it is today, and medical evacuation flights are an essential solution.

The risk for illness or injury remains high in all travel situations.

Almost any aircraft with minimal medical equipment can be described in loose terms as an air ambulance, especially when the government regulation of air ambulances is surprisingly limited. Costs, services and quality vary significantly. It is important to ascertain specifics about service, staffing, equipment, and expertise when selecting an air ambulance provider to ensure the patient's medical transport needs are met throughout the transport.

Repatriation Flights

The term *expatriate* is often used to describe a person who is temporarily or permanently residing in a foreign country. Usually this description does not encompass tourists or students traveling abroad, but it may be used when describing students who are studying abroad for extended periods of time. Derived from the word *repatriate,* the return of the person due to illness or injury by an air ambulance flight or a medical escort may be referred to as a *repatriation* flight. Repatriation is the process of returning assets that are held in foreign destinations to their home or place of origin. Medical transport refers to the transport of a patient from what is considered a foreign location to his or her home state, province, or country. While this term is used primarily when speaking of a foreign national, it may also be used to describe a domestic transport between one state and the patient's home state. Most of these transports are conducted in jet aircraft since they involve distances that often exceed the capabilities of helicopter transports, which are more commonly thought of by individuals when air ambulance is mentioned. Transport across international borders requires unique pre-transport preparations compared to transport involving domestic originations and destinations. The required preparation and planning is dependent on the length of the transport, the patient's condition, and the aircraft selected.

The proper aircraft selection is determined by the mission requirements and may involve aircraft ranging from those used primarily for executive charter, to those permanently equipped for air ambulance flights. Routinely, jet aircraft are used for transports exceeding 500 miles. For missions less than 500 miles, a twin-engine pressurized aircraft flown by two pilots would be appropriate. Executive charter aircraft are used for executive or private flights. Often the interiors of these aircraft are interchangeable between an executive configuration and an air ambulance configuration, and can be reconfigured within

a couple of hours. Transporting a patient on a commercial flight using medical escort(s) has its own specific intricacies, as it involves transporting the patient through airport terminals, providing care in the presence of the commercial aircraft population, and adhering to the established schedules of commercial carriers. By and large, the best choice for repatriation flights is a permanently equipped air ambulance aircraft. A true air ambulance aircraft has been reconfigured with an ICU-capable medical interior for the exclusive use of air ambulance operations.

Selecting a Reputable Medical Transport Service

There are several key factors to consider when selecting a company to transport your ill or injured traveler. First and foremost are the aviation accreditations and certificates held by the operator. Aircraft operators are required to hold a current Air Carrier Certificate (FAA document #8430) in accordance with Federal Aviation Regulations (FARs) regulated by the Federal Aviation Administration (FAA). In order to conduct air ambulance missions, the air carrier is required to operate under approved operations specifications, including those for air ambulance operation. These specifications regulate installed medical equipment (such as a stretcher in the aircraft). However, *portable* equipment, which may also include stretchers, is not regulated by these specifications. Moreover, the FAA chooses not to exercise control over the medical aspects of the flight, which include the medical staffing or equipment required for the flight. When selecting the aircraft and an air ambulance provider, one can easily determine that the service providing the flight is an approved air carrier and that the aircraft is operated within approved air ambulance operation specifications, simply by requesting and examining a copy of the operator's air carrier certificate.

The best choice for repatriation flights is a permanently equipped air ambulance aircraft.

In addition to the Air Carrier Certificate, the carrier must also maintain currency of several credentials and must have proof of these on hand, as they must be presented immediately upon request to demonstrate compliance with all federal regulations and other applicable international requirements. Several such documents are:

- Air Worthiness Certificate (FAA document 8100-2)
- Air Ambulance operations specifications
- Aircraft registration (FAA document #8050)
- Minimum Equipment Lists (MEL) as approved for the aircraft
- Minimum Navigation Performance Specifications (MNPS) and Reduced Vertical Separation Minimum (RVSM)
- Operations specifications as cited for the aircraft type (FAR 91.705/AC 91.49)
- Diplomatic clearance reference numbers and landing permit filings for all areas of operation
- Passenger Manifest
- General Declarations Record (U.S. Customs and Immigration)
- U.S. Customs Bond/Decal
- Documentation of U.S. TSA No-Fly Lists references

Additionally, to confirm coverage limits, the operator should also provide a certificate of insurance for the service's aircraft liability and professional liability, or a bond sufficient to meet the requirements of all U.S. agencies or foreign governments within their operation. For aircraft liability insurance, air ambulance operators are advised to carry a minimum of the following amounts for each aircraft: $5 million for twin engine aircraft; $10 million for turboprops; and $20 million for jets. For international providers, insurance requirements for the specific regions in which the aircraft is operated must also be considered. For example, to operate within European airspace, aircraft ranging from more than 26,400 pounds to 55,000 pounds in gross weight must carry €80 million minimum limits of liability, which amounts to slightly more than $117 million. Furthermore, a minimum of $1 million in medical malpractice insurance is recommended, and operating certificates and air ambulance permits for areas of operation must be maintained for places like Mexico, Canada, etc.

Other Considerations

The FAA regulations provide minimum requirements with which the operator must comply. The professionalism and

expertise of the provider may be determined by evaluating the program's achievement of specific benchmarks identified within the transport industry. One such benchmark that reflects the program's commitment to excellence is accreditation by the Commission of Accreditation of Medical Transport Systems (CAMTS). CAMTS offers a voluntary evaluation of compliance with accreditation standards, demonstrating the ability to deliver service of a specific quality. By participating in the voluntary accreditation process, services can illustrate their adherence to quality accreditation standards to their peers, medical professionals, and to the general public. Accredited programs are identified on the CAMTS website (www.camts.org), including the specific lines of business for which they are approved (e.g., international, fixed-wing, commercial medical escorts, etc.). Moreover, the air ambulance provider's experience can be ascertained with the provision of evidence demonstrating operational experience within each region.

A firm, itemized price quotation should be agreed upon between the customer and the provider prior to the transport, and should be provided to the customer in writing. Costs will vary depending on type of aircraft, mileage, flight dispatching cost, medical staff required by the patient, needed medical supplies, and ground ambulance charges. International and long-range domestic transports may be subject to additional costs such as foreign ground handling fees and taxes, overseas air traffic control charges, over-flight permits, crew overnight expenses, and relief pilot positioning via commercial airlines. The customer must verify which items, if any, are included in the price quotation.

Often the customer may contact an individual to obtain service, without realizing the individual is not part of an air ambulance provider's operation. A customer may also contact a company that appears to be an air ambulance provider, yet in reality does not own or operate aircraft at all. This company may then act as a broker on the customer's behalf by seeking an ambulance program to provide the service—but charge the costs (in addition to a broker fee) to the customer. Brokers may be helpful if the customer is not familiar with how to locate, interview, and hire a reputable air ambulance provider. But caution should be taken when using a broker for medical transports, as determining the quality of service and who will actually be providing it is difficult at best. When a company's status is questionable, inquire as to whether it holds an Air Carrier Operating Certificate.

When a company's status is questionable, inquire as to whether it holds an Air Carrier Operating Certificate.

Experienced air ambulance providers will proficiently plan for the following logistical considerations as applicable when conducting patient transports internationally:

- Communication with the aircraft, since in-flight phone systems will not operate outside the U.S. and cellular coverage is limited in foreign locations
- Language barriers in some international locations, and how to overcome these barriers
- Arrangement of ground ambulances, and possible differences between domestic and foreign ground services
- Entry and exit documents for the flight crew, medical crew, patient, and all passengers onboard the aircraft for each international stop during the flight (including all technical or aircraft refueling stops of the aircraft). Some or all of the following may be requested depending on the governmental regulations specified for that particular country or region:
  - Passports
  - Visas
  - Proof of citizenship
  - Crew photos and licensure (flight crew and medical professionals)
  - Declaration and immigration forms for crew and passengers
  - Internationally approved immunization records or documentation (for specific information, please refer to the World Health Organization at www.who.int and/or Centers for Disease Control at www.cdc.gov/travel)

Not having the documents as requested may result in fines or citations, civil and/or criminal penalties, or even denial of entry or exit in certain countries. Flight crews with proper ID are exempt from many of these regulations, but exemptions vary between foreign destinations.

Medical teams are not recognized as flight crew in many areas and should be prepared to present as many of the requested documents as possible.

Pre-departure communication directly between the transferring facility, receiving facility, and the transport team is essential to obtain a clear and accurate evaluation of the clinical status of the patient. Language barriers may cause difficulties in receiving accurate patient information prior to arrival. Many air ambulance providers skilled in international medical transports have discovered that the use of bilingual medical team members provides an effective communication tool and eases the challenges often experienced when working with differing cultures and foreign locations. The use of interpreters may be beneficial, especially if they are local to the transferring facility. Language barriers must be addressed and all necessary arrangements made to facilitate the transfer of care from the treating professionals to the transport medical team without any disruption in the treatment plan.

In addition, pre-departure communication must also include confirmation of the accepting physician and bed assignment at the receiving facility. Pre-admission information provided prior to the patient's arrival may also ease the transition during transfer of care. Preparation by the receiving facility to provide apposite care depends on the communication received from the transferring facility and the transport medical team in preparation for the patient's arrival. Frequent communication during the transport by the medical team is also essential for providing the receiving professionals with updates on the patient's condition, for making necessary provisions to minimize changes in treatment regimens, and for facilitating the transfer of care upon arrival to the receiving facility. Communication may be enhanced with the use of satellite telephones and by implementing procedures that require the medical team to call the receiving facility during the scheduled technical stops of the aircraft.

The ground transport between the aircraft and the referring and treating facilities poses the most risk for the patient due to the possible lack of medical supplies and oxygen; incompatibility of medical equipment, electrical power, oxygen delivery systems and adapters; or insufficient training by the ground ambulance provider. It is imperative that accommodations be made by the air transport service to minimize these risks. Accompanying the patient to the hospital on the ground unit and using the service's own medical transport equipment during the ground transport phase may help. This is commonly described as a bedside-to-bedside transport, where the provider insures continuity of care for the patient and compliance with federal laws that regulate the level of care provided. Plans must also be made for powering the equipment, servicing and administering the oxygen, and operating suction and monitoring devices that allow normal operations throughout every aspect of the transport. These provisions may require the use of the medical team's portable oxygen systems, battery-powered suction units, transport monitor, and transport ventilator.

Duty time of the medical team is equally important for safe, quality patient care.

Lastly, practiced international air ambulance providers have established alternative plans to allow for the removal and transfer of the patient to an interim facility, if the medical team or aircraft is not appropriately equipped to provide optimal care. This may become necessary if the patient's condition deteriorates during flight, or if the aircraft or an essential piece of medical equipment experiences a mechanical failure.

Crew Duty and Rest Requirements

Compliance with FAA flight crew duty-time regulations necessitates assiduous flight planning and strategic crew positioning to complete each flight without interruption, and to provide required rest for the crew prior to the aircraft arrival.

Duty time of the medical team is equally important for safe, quality patient care, so rest periods must be allowed. On transports involving extended patient care times, positioning medical team members and transferring care during the aircraft technical stop may be required.

In addition to duty-time provisions, travel arrangements and accommodations must also be considered for safe travel of the flight and medical crews. Providers may employ agencies to monitor travel warnings and to

assist with the safe travel of their crews. At the very least, systematic monitoring of resources (such as the U.S. State Department's lists of travel warnings and safe travel practices) is necessary to insure the team's safety at all times. Reputable air ambulance programs adhere to all of these regulations.

Medical Crew Staffing and Equipment

All medical staff should be appropriately licensed, age-specific Advance Cardiac Life Support (ACLS) certified, and current in their specialty. All medical personnel must have training in altitude physiology, infection control, stress recognition and management; patient care capabilities and limitations during transport; and aircraft safety procedures, including depressurization.

When selecting the medical team for a particular flight, the needs of the patient, requests of the transferring and receiving facilities and physicians, length of the transport, and cross-cultural team composition must be considered. For example, some cultures do not recognize the expertise of critical care or flight nurses and/or paramedics. Many fixed-wing air ambulance providers replace the more traditional nurse/paramedic flight team with nurse/respiratory therapist teams, especially on transports involving ventilator-dependent patients. Physicians may also complement the team for patients requiring a certain level of care during transport, or at the request of the treating and receiving physician. Team members should be selected based on their level of skill and should augment the other team members' expertise. Although medical staffing for a transport should be made in conjunction with the client's medical department, the final determination of an appropriate staff rests with the air ambulance provider. A minimum of two medical personnel is recommended for all air ambulance flights. It is essential that the medical team configuration be planned to account for changes in the patient's condition during the transport.

A minimum of two medical personnel is recommended for all air ambulance flights.

Meticulous planning is required for any long-range flight, but especially for transports involving international operations. Lengthy patient care times are correlated with such transports, as are extended periods of time outside a major medical facility. Preparations for adequate medical supplies, medications, and, most importantly, oxygen must be arranged to meet the patient's needs for the duration of the transport, with consideration to any potential delays that might be experienced. The medical team must be familiar with and diligently monitor the battery life of essential equipment and available supply of medical gases throughout the transport.

Conclusion

Air medical evacuations require conscientious planning, especially when such transports involve extended times outside a medical facility or traverse international boundaries. The safety of the flight and medical crew, the patient, and all passengers is integral to the planning process and must remain the priority throughout all phases of transport. Knowing the facts will prepare you for the selection process when an air ambulance is needed.

About the Author

Denise Treadwell, CRNP, MSN, CEN, CFRN, CMTE is Executive Vice President for AirMed International. She is internationally recognized as one the top transport nurses in the field of air medical transports, having participated in hundreds of missions to six continents. At AirMed, the country's leading fixed-wing air ambulance company, she is responsible for managing 50 medical professionals, including trauma and emergency physicians, emergency and critical care trained nurses, respiratory therapists, and paramedics. Her experience was instrumental in developing AirMed's emergency response procedures for medical evacuation services. Ms. Treadwell is the past president of the Air and Surface Transport Nurses Association; an active member of the Emergency Nurses Association; and an interim instructor for the Nurse Practitioner and Advanced Paramedic courses at the University of Alabama at Birmingham (UAB). She holds two masters' degrees in trauma nursing and family nurse practitioner from UAB.

References

Federal Aviation Administration: *Federal Aviation Regulations*. Available at www.faa.gov.

Federal Aviation Administration: *International Flight Information Manual*. Available at www.faa.gov/ats/aat/ifim.

Federal Aviation Administration: *Notices to Airmen (NOTAMS)*. Available at www.faa.gov/NTAP.

Federal Aviation Administration: *Minimum Navigation Performance Specifications*. Available at www.faa.gov/ats/aat/ifim/ifim0108.htm.

Federal Aviation Administration: *Reduced Vertical Separation Minimum*. Available at www.faa.gov/ats/ato/rvsm1.htm.

U.S. Department of Homeland Security: *Transportation Security Administration*. Available at www.tsa.gov/public.

U.S. Department of Homeland Security. Available at www.dhs.gov/dhspublic.

U.S. State Department. Available at www.state.gov.

Centers for Disease Control and Prevention: *Travelers' Health Team*. Division of Global Migration and Quarantine. Available at www.cdc.gov.travel.

World Health Organization: *Health Topics: Immunizations*. Available at www.who.int.

Holleran, R. S. *Flight Nursing: Principles and Practice*. 3rd ed. St. Louis: Mosby, 2003.

Treadwell, D. *Standards for Critical Care and Specialty Fixed-Wing Transport*. Denver: Air & Surface Transport Nurses Association, 2004.

Holdefer, W. F., D. Treadwell, and J. T. Tolbert. "International air medical transport, program profile." *International Air Ambulance* 7 (1998): 36.

Holdefer, W. F., D. Treadwell, and J. T. Tolbert. "International air medical transport ventilator dependent patients." *International Air Ambulance* 9 (1999): 22.

If earth in any quarter quakes

Or pestilence its ravage makes,

Thither I fly.

—John H. Finley (1863–1940), "The Red Cross Spirit Speaks"

In cases of defense 'tis best to weigh

The enemy more mighty than he seems.

—William Shakespeare (1564–1616), *Henry V,* Act II, Scene 4

The Mixed Motive Instruction in Employment Discrimination Cases: What Employers Need to Know

David Sherwyn, J.D., Steven Carvell, Ph.D., Joseph Baumgarten, J.D.

Abstract: In litigation regarding employment discrimination, the burden of establishing proof has continued to shift. As a result, employers and legal counsel need to be aware of the status of what they and human resources professionals should consider when an employee alleges that the employer has violated federal discrimination statutes. The original standard of proof required the plaintiff to establish that the employer discriminated against that person. Many cases still involve that approach, giving the plaintiff the burden of creating a prima facie case. *However, another line of rulings by the U.S. Supreme Court added an alternative method for addressing discrimination litigation, known as the mixed motive approach. The two-prong mixed motive case requires the employee to demonstrate that a protected characteristic (e.g., race, sex, national origin) was a substantial factor in an employer's adverse action. If that is established, the employer then has the burden of proving that the decision would have been made in any event, regardless of the employee's protected characteristic. As a practical matter, employers facing litigation of this type must consider whether and how to defend such a case. Even a "win" can be expensive, because in cases where there is a divided decision, the employer must pay the plaintiff's attorney fees and court costs, as well as its own. Moreover, since the Civil Rights Act of 1991 places discrimination cases in front of a jury, a divided decision is seemingly more likely. Although that presumably gives both sides a win, it still means a large expense for the employer.*

The burden of proof in discrimination cases has been the subject of at least eight Supreme Court cases, hundreds of lower courts cases, and thousands of law review pages. Some might consider the time spent on this topic to be a prime example of a situation in which the Supreme Court, numerous lower court judges, lawyers, and academics are focusing too much energy on a relatively meaningless question. The issue is not meaningless to those who have found themselves the target of litigation, however. For those parties, the way that courts assign the burden of proof may, in fact, determine the probability of a damage award and the amounts of the damages awarded. Thus, a change in the allocation of the burden of proof can affect the number of cases filed, the amount of settlements agreed upon, and the fate of thousands of cases.

A change in the allocation of the burden of proof can affect the number of cases filed.

In contrast to the view that burden of proof is immaterial, we note the holding in *Desert Palace d/b/a Caesars Palace Hotel & Casino v. Costa*. In this opinion, the United States Supreme Court set a new standard for determining whether plaintiffs can get a "mixed motive" jury instruction in discrimination cases.[1] This case represents a major shift in the balance of power in discrimination lawsuits. In fact, as we explain below, it is possible that *Costa*'s effect will be so great that employers should rarely go to trial in discrimination cases because the cost of losing will be so high and the odds of winning so low. Knowing this, plaintiffs' lawyers will be apt to take increasingly marginal cases and will demand higher settlements. If our analysis is correct, *Costa* will have fundamentally changed the face of discrimination cases by transforming marginal cases into huge liabilities for employers.

In this report we analyze the effect of the shifting burden of proof, particularly in the wake of *Costa*. Unfortunately, as we explain below, neither an analysis of published legal opinions nor any other traditional method of legal research will answer the question. Because the precedent in *Costa* is relatively recent, a survey of lawyers is unlikely to answer this question with any certainty. Thus, to analyze the effect of *Costa*, we have developed our

own data from a test sample. In addition to a discussion of the cases leading up to the *Costa* holding, this Center Report presents the results of a study that we conducted to determine the effect of *Costa* on the outcome of discrimination cases. Our discussion of *Costa* begins with an examination of burden of proof, describes the two different methods of proof in discrimination cases, clarifies how these two methods of proof have developed, and sets forth the employer's options in discrimination cases.

Understanding the Burden of Proof

To understand the two different methods for proving discrimination, it is necessary to explain how burdens of proof work. When a case reaches the trial stage, one party bears the burden of proof, and therefore must convince the factfinder that its position is correct. In contrast, the other side need not prove anything. As a result, the primary task of the party without the burden is to prevent the other side from proving its argument. To better understand the concept of burden of proof, imagine a football field. The job of the offense is to score and the defense's job is to prevent the offense from scoring. In a legal context, the side with the burden of proof is the offense, with the other side being the defense. While it would be nice for the defense to score, it does not have to. Similarly, while it would be nice for the litigant without the burden of proof to prove its case, it does not have to. It simply must prevent the other side from meeting its burden.

Depending on the type of litigation, the party with the burden of proof will face one of three standards of proof. Those are (1) preponderance of the evidence, (2) clear and convincing evidence, and (3) beyond a reasonable doubt. Continuing the football analogy, to satisfy the preponderance standard, the "offense" must get the ball past the fifty-yard line into the other team's territory. The clear and convincing standard requires the ball to fall within easy field-goal range near the goal line. Last, establishing a case beyond a reasonable doubt is comparable to a touchdown, in that the factfinder must be almost certain of the facts being adduced.

An effective way to explain the operation of the burden is to look at one of more famous criminal cases of the 20th century: *People of California v. O. J. Simpson*. In *Simpson*, as in all criminal cases, the prosecution carried the burden of proving "beyond a reasonable doubt" that Simpson was guilty of murder. The defense, on the other hand, was not required to prove anything. For instance, Simpson needed neither to prove that he did not kill the victims nor did he need to prove that someone else did. Rather, Simpson simply had to prevent the prosecution from successfully proving its case by attacking the prosecution's assertions. For example, the prosecution presented blood from the crime scene, claiming it belonged to Simpson. Instead of proving that the blood did not match his, however, Simpson merely presented evidence to show that the chain of custody was broken, and therefore the evidence was unreliable. When the prosecution presented bloody gloves, Simpson discredited this evidence by demonstrating that the gloves did not fit him. Again, Simpson only needed to attack the prosecution's evidence; he never had to prove his innocence.[2]

Why a Case's Outcome May Depend on Burden of Proof

There are two methods for proving intentional employment discrimination: (1) the *McDonnell Douglas* method; and (2) the "mixed motive" method. Based on the circumstances of the case, the judge determines whether to classify a matter as being a "mixed motive" case.

McDonnell Douglas: Burdening the Plaintiff

In *McDonnell Douglas Corp. v. Green*, the Supreme Court set forth a standard of proving discrimination in which the burden of proof remained with the plaintiff at all times.[3] Under the *McDonnell Douglas* approach, plaintiffs must first prove a "*prima facie* case" by showing that they: (1) are members of a protected class; (2) were minimally qualified and either applied for or held the job; (3) suffered an adverse employment action; and (4) either the job remained open, was filled by someone outside the class, or similarly situated employees outside the protected class engaged in similar conduct and did not suffer the same adverse action. Plaintiffs that prove these four elements, which typically are not difficult to establish, create a presumption of discrimination. The defendant must then rebut this presumption.

In *Texas Department of Community Affairs v. Burdine*, the Supreme Court "clarified" how employers may rebut the presumption created when the plaintiff proves a *prima facie* case.[4] *Burdine* held that the employer does not have

to prove that it hired the best applicant or that it did not discriminate. Instead, the employer only has the burden of "articulating" a non-discriminatory reason for the employment decision. This requirement is not, however, a burden of proof. Instead, the employer's burden is merely one of production. The employer must set forth the reason for its decision, but need not prove that the reason given is true. If the employer indeed satisfies its burden of production, the employee, according to *Burdine*, could then take further steps to prove discrimination in one of two ways. First, the plaintiff can prevail by demonstrating that the real reason for the decision was discrimination (notwithstanding the reason given by the employer). Alternatively, the plaintiff could prevail by proving that the reason articulated by the employer was pretext (unworthy of belief). In either situation, the plaintiff, according *Burdine*, would prevail as a matter of law.

The mixed motive instruction was only available when the employee had direct evidence of discrimination.

Mixed Motive: The Burden Begins to Shift

Seven years after *Burdine*, in *Price-Waterhouse v. Hopkins,* the Supreme Court developed a second method for proving intentional discrimination.[5] This method is referred to as the "mixed motive" method. In *Hopkins*, the plaintiff alleged she was denied partnership at Price-Waterhouse because she was a woman. To prove her case, the plaintiff presented evidence that partners made a number of discriminatory comments to her, including statements that she: (1) "was too masculine"; (2) "should wear more make-up"; and (3) "should go to charm school." The Court held that basing employment decisions on a failure to live up to a sexual stereotype constituted discrimination. Accordingly, the plaintiff would prevail if the employer relied on these discriminatory reasons for denying Hopkins partnership. The employer did not deny the alleged discriminatory reasons, but presented additional reasons for the decision not to promote the plaintiff. For example, the employer presented evidence that the plaintiff was disliked by staff members and had difficulty getting along with colleagues. In addition, the employer argued that it previously denied partnership to male employees with deficiencies similar to those of the plaintiff.

The *Hopkins* Court was presented with a peculiar set of circumstances. Because there were both legitimate and illegitimate reasons for the employer's decision, the Court held that the *McDonnell-Douglas* method was not appropriate for resolving the case. In a hotly contested split decision, Justice O'Connor's concurring opinion, which most courts accept as the case's holding, set forth a new standard of proof for so-called "mixed motive" cases. Under O'Connor's opinion, the mixed motive standard of proof requires an employee to prove by "direct evidence" that the protected characteristic, such as sex, was a substantial factor in the employer's decision-making process. If the employee fails to meet this burden, the case is over. If, however, the employee satisfies the substantial factor test, the burden of proof shifts to the employer, which now has to prove (rather than merely assert) that it would have made the same decision regardless of the employee's protected characteristic. An employer who meets this burden avoids liability and precludes the plaintiff from receiving an award. Conversely, if the employer fails to prove it would have made the same decision regardless of the protected characteristic, the plaintiff receives back pay, reinstatement, attorney's fees, and litigation costs.

O'Connor's opinion emphasized that the mixed motive instruction was only available when the employee had direct evidence of discrimination. Examples of direct evidence include statements, documents, or other tangible examples of discrimination. Alternatively, circumstantial evidence, which consists of facts put together to create an inference of discrimination, did not entitle a plaintiff to a mixed motive method of proof.

How *Hicks* Confused Matters

With its shifting burdens of proof, *Hopkins* created a model that was easy to follow. Employees with direct evidence of discrimination could argue their case was a "mixed motive" case and shift the burden of proof onto the employer. On the other hand, if there was no direct evidence of discrimination, plaintiffs would be required to prevail under the *McDonnell Douglas* formula. This "nice

and neat" model lost some of its appeal after the Supreme Court decided *St. Mary's Honor Center v. Hicks*.[6]

In *Hicks*, the plaintiff proved that the employer's stated reason for terminating the employee was a pretext. The Court of Appeals for the Eighth Circuit held that proving pretext entitled the plaintiff to a judgment as a matter of law. The Supreme Court, however, reversed the Eighth Circuit and held that while factfinders may infer discrimination from a finding of pretext, plaintiffs are entitled to judgment as a matter of law only if they prove both that an employer's articulated reason was a pretext and also that the real reason for the decision was discrimination. Commentators refer to this standard as "pretext plus evidence," or, more simply, "pretext plus." Not surprisingly, plaintiffs' advocates were outraged by this holding, while those representing management were delighted by the decisions.[7]

Although a discussion of the merits of *Hicks* is beyond the scope of this report, its effect on discrimination litigation is profound and must be addressed. Before *Hicks*, the two different burdens of proof created a simple coherent model. Employees with no direct evidence of discrimination used the *McDonnell Douglas* formula and employees with direct evidence asked the court to consider the case to be mixed motive. After *Hicks*, cases without evidence were considered "orphan" cases.[8] Plaintiffs' lawyers did not want to invest years of time and money into a case that required a factfinder to infer discrimination. Instead, it made more sense to take on only those cases with actual evidence.[9] If there was direct evidence, plaintiffs' lawyers would contend that they were entitled to a mixed motive instruction. Still, a model did survive: direct evidence involved *St. Mary's v. Hicks*, while circumstantial evidence invoked *McDonnell Douglas*.

The passage of the Civil Rights Act of 1991 drastically changed the mixed motive landscape.

Civil Rights Act of 1991: More Complications

While the formulas of proof were important, their real effect was limited for the following two reasons. First, Title VII of the Civil Rights Act of 1964 (CRA) did not permit jury trials.[10] Second, under *Hopkins* employers could prevail in mixed motive cases by proving they would have made the same decision regardless of the plaintiff's being part of a protected class. Accordingly, even though the mixed motive method redirected the burden of proof, employers could still prevail if they were able to convince the judge that they had not discriminated. The passage of the Civil Rights Act of 1991 drastically changed the mixed motive landscape by: (1) allowing jury trials in Title VII cases,[11] and (2) changing the standards and damage scheme for mixed motive cases.

Before jury trials were permitted in Title VII cases, judges were the factfinders in cases relating to discrimination by race, sex, color, religion, and national origin. In many of these cases, the plaintiffs' lawyers would argue that the case was a mixed motive case and the employer would argue it was not. A judge who was unsure whether the case warranted applying the mixed motive method could appease the plaintiff and prevent a successful appeal by labeling the case "mixed motive" but then holding that the employer satisfied its burden.

Charging the jury

After the CRA of 1991, however, the question of whether a case warranted application of the mixed motive method had a profound effect on the matter of who would be the factfinder. From that point on, the judge's decision regarding whether the case is to be decided according to the *McDonnell Douglas* rules or the mixed motive approach manifests itself in instructions to a jury. A judge who labels a case as being a mixed motive case must instruct the jury that the employer must prove that it did not discriminate. Because of the difficulty of proving a negative, whether the judge instructs the jury with a mixed motive standard rather than a *McDonnell Douglas* standard may determine the result of the case. Placing the burden of proof on employers leads one to believe that employers will find it difficult—perhaps impossible—to prevail in mixed motive cases, especially given the perception that juries favor employees over employers.[12]

To make matters worse for employers, the CRA of 1991 made the mixed motive instruction more "plaintiff friendly" in the following two essential ways. First, the statute made it easier for a plaintiff to obtain the judge's determination that the case involved a mixed motive. Under CRA of 1991 plaintiffs no longer have to prove

that the protected characteristic was a substantial factor in the employer's decision. Instead, the new standard is that the protected characteristic be a "motivating factor" in the employment decision, which is an easier test to satisfy.

Second, the act changed the damage scheme to the point where litigating these cases becomes foolish for employers. We make this conclusion because judges can now award attorney fees, litigation costs, and declaratory judgments to plaintiffs who met the "motivating factor" standard, even where the employer meets its burden of proving that the decision would have been made anyway. Thus, employers who successfully prove that the business decision would have been made regardless of discrimination are still subject to huge expenses and damages.

The effect of awarding costs and fees is profound because they are the major damage component of most discrimination cases. In large cities like New York and Chicago, management lawyers report that their fees for a discrimination case will almost always exceed $150,000 and have often been well over $500,000.[13] While plaintiffs' lawyers' fees awards are almost always less than management's fees, they are still considerable. After the CRA of 1991, mixed motive cases became costly because employers who "won" still might have to pay their attorneys' fees and often the plaintiff's fees. Accordingly, it could easily cost an employer over $500,000 to "win" a mixed motive case. This figure does not include out-of-pocket litigation expenses for each side, lost employee and management time, and the bad publicity that accompanies both the trial and subsequent judgment of discrimination. As a result, after 1991 employers were well advised to settle mixed motive cases, because the costs of "winning" would almost always greatly exceed the settlement demand.

After 1991 employers were well advised to settle mixed motive cases.

The solace for employers was that mixed motive instructions were relatively unusual. The majority of jurisdictions held that a mixed motive instruction would only be given in cases with direct evidence of discrimination, which is hard to come by. Indeed, decision makers rarely make discriminatory remarks in writing or in front of employees who might testify against the company. Thus, the mixed motive instruction was unavailable in the most discrimination cases.

How *Costa* Redefined the Landscape

Returning to the case originally known as *Costa v. Desert Palace*, the Ninth Circuit diverged from other circuits by holding that either direct or circumstantial evidence was sufficient to warrant a mixed motive instruction. To resolve the split among the circuits, the Supreme Court agreed to hear the case, issuing its decision in 2003, as *Desert Palace d/b/a Caesars Palace Hotel & Casino v. Costa*.[14] The issue in *Costa* was whether direct evidence of discrimination was required for a plaintiff to receive a mixed motive instruction or whether circumstantial evidence would suffice.

In arguing for direct evidence, the employer in *Costa* contended that Justice O'Connor's concurring opinion in *Hopkins*, which required direct evidence, was the holding of the case and still the law. The plaintiff, on the other hand, argued the CRA of 1991's language was clear and did not require any specific type of evidence. Rather, it merely stated that the plaintiff had to prove that discrimination motivated the employer.

In a unanimous decision, the Court held that the CRA of 1991's language was unambiguous and did not require direct evidence. Thus, any type of evidence of discrimination may enable a plaintiff to receive a mixed motive instruction. This decision could change the face of discrimination law because a plaintiff with any evidence of discrimination can now receive a mixed motive jury instruction, which, as we said above, may be tantamount to winning the case.

The Mixed Motive Instruction versus the Pretext Instruction

To clarify this distinction, let's compare a sample mixed motive instruction with a typical pretext instruction. Each court may fashion its own specific jury instructions, as long as they are in accordance with settled law. Some jurisdictions, however, established model jury instructions that are used in the most cases. These instructions are accompanied by what are referred to as "special jury verdict sheets." With that caveat, the pages to follow give sample instructions from the United States Court of Appeals for the Seventh Circuit and sample special verdict sheets.

The difference between the two instructions may seem minimal and meaningless, but the difference is large when one considers the contention made several years ago by film director Spike Lee, who stated that race motivates a part of every decision. Regardless of whether Lee was correct, it is possible that a substantial number of potential jurors agree with him. It is also possible that there are those who feel the same way about sex, color, national origin, religion, age, and disability. Lee's contention is important because anyone who subscribes to this theory will find that virtually any plaintiff in a discrimination case has satisfied the initial burden in the mixed motive scheme. The problem with that observation, however, is that after the CRA of 1991, the employee would receive costs and attorney fees based on nothing more than that determination, even if the jury then decided that the employer's decision would have been the same if race or other protected classes were not involved. This situation infuriates management lawyers. Jurors do not know that their belief that discriminatory factors always motivate decisions means that they will unwittingly award the plaintiff costs and fees, regardless of the employer's intentions.

A Comparison of Jury Instructions in a Failure-to-promote Case Based on National Origin

"Pretext" Instruction:

Plaintiff bases his lawsuit on Title VII of the Civil Rights Act of 1964, a law that makes it unlawful for an employer to discriminate against an employee on the basis of national origin. To succeed on this claim, Plaintiff must prove by a preponderance of the evidence that he was denied a promotion by Defendant because of his national origin.* To determine that Plaintiff was denied a promotion because of his national origin, you must decide that Defendant would have promoted Plaintiff had he not been of his particular national origin but everything else was the same.

If you find that Plaintiff has proved by a preponderance of the evidence each of the things required of him, then you must find for Plaintiff. However, if you find that Plaintiff did not prove by a preponderance of the evidence each of the things required of him, then you must find for Defendant.

"Mixed Motive" Instruction:

Plaintiff bases his lawsuit on Title VII of the Civil Rights Act of 1964, a law that makes it unlawful for an employer to discriminate against an employee on the basis of national origin. To succeed on this claim, Plaintiff must prove by a preponderance of the evidence that his national origin was a motivating factor in Defendant's decision not to offer him a promotion. A motivating factor is something that contributed to Defendant's decision.

If you find that Plaintiff has proved that his national origin contributed to Defendant's decision not to offer him a promotion, you must then decide whether Defendant proved by a preponderance of the evidence that it would have not offered him a promotion even if Plaintiff was not of his particular national origin. If you find that the Defendant has proven that it would not have offered him a promotion even in the absence of discrimination, you must still enter a verdict for the Plaintiff but you may not award him damages.

Special Verdict Sheets

Pretext Cases:

1. Did plaintiff establish by a preponderance of the evidence that defendant discriminated against him in violation of Title VII of the Civil Rights Act of 1964 on the basis of his national origin with respect to the decision not to offer him a promotion in December 2003?

   Yes ____ No ____

   If you answered "no" to Question 1, sign the special verdict form on the last page. If you answered "yes" to Question 1, plaintiff is entitled to recover back pay damages. The parties have stipulated that the total amount of back pay to be awarded to plaintiff is $50,000. Check the box below to signify that the plaintiff is entitled to damages of $50,000 and then sign the special verdict form.

Mixed Motive Cases:

1. Did plaintiff establish by a preponderance of the evidence that his national origin was a motivating factor in the decision by defendant not to offer him a promotion in December 2003?

   Yes ____ No ____

   You should answer the next question *only* if you answered "yes" to Question 1. If you answered Question 1 "no," you should not answer any further questions but sign

this special verdict form on the last page and return the form to the clerk.

2. Did defendant establish by a preponderance of the evidence that the defendant would have treated plaintiff the same way even if the plaintiff's national origin had not played any role in the employment decision?

   Yes ____ No ____

   If you answered "yes" to Question 2, sign the special verdict form on the last page. If you answered "no" to Question 2, plaintiff is entitled to recover back pay damages. The parties have stipulated that the total amount of back pay to be awarded to plaintiff is $50,000. Check the box below to signify that the plaintiff is entitled to damages of $50,000 and then sign the special verdict form.

** Our example involves national origin, but it could be any of the other six protected classes: namely, sex, race color, religion, age, or disability.*

One "Management Lawyer's" Method for Avoiding the Unintended Fees

Considering this two-part test, coauthor Joe Baumgarten, of the law firm of Proskauer, Rose, raised another concern. He hypothesized that to suit their sense of "fair play," juries that are presented with a two-prong decision would "split the baby," as follows. They first would hold that the protected class motivated the employer. Then they would determine that the employer would have made the same decision regardless of the protected class. Once again, such a jury would have no idea that it had just awarded costs and fees to the plaintiff. Baumgarten sought to eliminate this problem by taking the issues in stepwise fashion. Rather than offer both prongs of the mixed motive instruction, Baumgarten suggests simply having the jury determine whether the protected class motivated the employer's decision. He argues that a jury might be less inclined to find such motivation if that is the only question asked and if they knew that the finding of "yes" meant that the employer had to pay damages. Because the second prong involves an employer's defense, the employer can determine in advance whether to present it. Thus, Baumgarten proposed a third set of instructions and special jury verdict sheet. In this instruction he eliminated the second prong of the mixed motive instruction and the second question on the special verdict sheet. Thus, the instruction and the verdict sheet would appear as shown at upper right.

Alternative Jury Instruction

Mixed Motive Instruction without the "Second Prong"

Plaintiff bases his lawsuit on Title VII of the Civil Rights Act of 1964, a law that makes it unlawful for an employer to discriminate against an employee on the basis of national origin. To succeed on this claim, Plaintiff must prove by a preponderance of the evidence that his national origin was a motivating factor in Defendant's decision not to offer him a promotion. A motivating factor is something that contributed to Defendant's decision.

If you find that Plaintiff has proved that his national origin contributed to Defendant's decision not to offer him a promotion, you must enter a verdict for the Plaintiff, even if you believe that there were other motivating factors that would have caused the Defendant not to offer him a promotion even in the absence of any discriminatory motivation.

Special Verdict Sheet without the Second Question

1. Did plaintiff establish by a preponderance of the evidence that his national origin was a motivating factor in the decision by defendant not to offer him a promotion in December 2003?

   Yes ____ No ____

   If you answered "yes" to Question 1, plaintiff is entitled to recover back pay damages. The parties have stipulated that the total amount of back pay to be awarded to plaintiff is $50,000. Check the box below to signify that the plaintiff is entitled to damages of $50,000 and then sign the special verdict form.

What Does This All Mean for Employers?

Although courts are still divided on whether the pretext jury instruction is dead, it is clear that after *Costa*, more and more cases will receive mixed motive instructions. Consequently, employers need to know how to deal with this situation. Beyond that, we must examine whether the judge's instructions to the jury matter or whether certain language in the instructions has led to cases being settled for an amount greater than might otherwise occur. Then there's the question we raised at the beginning of this report, of whether employers should forget litigation and settle all mixed motive cases. If not, should employers use

Exhibit 1

Mixed Motive (MM) versus Pretext (P) Decisions

Not promoted because of national origin or national origin not a motivating factor		GROUP MM	GROUP P	Total
No	Count	42	57	99
	Expected Count	52.3	46.8	99.0
Yes	Count	34	11	45
	Expected Count	23.8	21.3	45.0
Total	Count	76	68	144
	Expected Count	76.0	68.0	144.0

	Value	Asymp.Sig. (2-sided)
Pearson Chi-Square*	13.626*	.01
w/ Continuity Correction*	12.329	.01
Likelihood Ratio	14.167	.01
Linear-by-Linear Association	13.531	.01

Notes: Pearson Chi-Square and continuity correction are computed only for a 2x2 table; N of valid cases = 144.

Exhibit 1A

Mixed Motive with Affirm Defense (MM w/AD) versus Pretext (P) Decisions

Not promoted because of national origin		GROUP MM *w* AD	GROUP P	Total
No	Count	70	57	127
	Expected Count	67.0	60.0	127.0
Yes	Count	6	11	17
	Expected Count	9.0	8.0	17.0
Total	Count	76	68	144
	Expected Count	76.0	68.0	144.0

	Value	Asymp.Sig. (2-sided)
Pearson Chi-Square*	2.364*	.124
w/ Continuity Correction*	1.636	.201
Likelihood Ratio	2.381	.123
Linear-by-Linear Association	2.348	.125

Notes: Pearson Chi-Square and continuity correction are computed only for a 2x2 table; N of valid cases = 144.

** Our example involves national origin, but it could be any of the other six protected classes: namely, sex, race color, religion, age, or disability.*

the Baumgarten rule and eliminate the second prong?

None of these issues can be resolved definitively, due to the pervasive problems associated with trying to use testing techniques common in social science to answer legal questions, as well as certain problems that are specific to the matter of jury instructions. Whenever legal scholars seek to answer questions using research methods from social science they battle a number of issues. First, not all cases are reported and those that are reported do not reflect a random sample. Second, even if all cases were reported there is still a problem when trying to draw specific conclusions from different cases with different sets of facts and different issues of law.

The issues we discussed here face even more problems than those related to sampling and idiosyncrasy. First, most settlements are confidential, making it essentially impossible to measure the effect of *Costa* on settlement size. Second, while a large number of discrimination opinions are published, the results of jury trials are not the issues that make it into the court reports. Instead, most of the reported cases feature the judges' opinions on summary judgment motions (which occur before the case goes to a jury) and appeals. The appeals cases are only relevant if the type of jury instruction is the issue being examined (a small percentage of appeals). Finally, looking at the results of jury trials is not helpful because the jury instructions are often not available so it is often impossible to know whether the case was a mixed motive case.

Experimental Testing Methodology

Since no data are available to answer the questions we have sought to address here, we conducted an experiment. Like many large law firms, Proskauer occasionally tests a case on a mock jury before the case goes to trial. Because of the cost of a full mock trial, however, Baumgarten and his team of lawyers sometimes test their case by having the mock jury hear a statement of the case only, rather than mock testimony or other evidence. Proskauer refers to these statements, which are combinations of an opening statement and closing argument, as "clopenings." Armed with the clopenings from the plaintiff and the defense on a sample case, we were able to conduct our experiment.

First, Proskauer videotaped two of its lawyers delivering the clopenings. Next, Proskauer videotaped Baumgarten delivering the following three different jury

instructions: (1) pretext instructions; (2) the two-prong mixed motive instruction, with the affirmative defense; and (3) the single-prong mixed motive instruction, without the affirmative defense. Armed with the tapes, we had to then find potential jurors. Unfortunately, the same people who will happily watch a *Law and Order* marathon are reluctant to take part in a law-related study. Thus, we asked students attending Cornell University to be our mock court jurors.

Study Design

We designed our controlled study as follows. On three separate nights, we had between 50 and 100 students sit in a particular auditorium and watch the clopenings, for a total of 219 students. We then randomly assigned each student to one of three roughly equal groups, each of which heard one of the test jury instructions. One group of 76 students was labeled MM, for mixed motive (the full, two-prong test); a second group of 75 students was called MMWO, for mixed motive without the affirmative defense (the single-prong idea); and the third, comprising 68 participants, was group P, for pretext. After hearing the jury instructions, each student received and filled out the designated jury verdict sheet. Like actual jurors, the MM students did not know that if they answered yes to question one and yes to question two they were awarding costs and fees. Again like actual juries, the MMWO and the P students, on the other hand, knew that they were awarding all or nothing based on their answer to the one question on their verdict sheet.

The results were remarkable. Before we discuss those results, however, we must add the caveat that we make no claim that our sample is representative of the juror pool at large. First, our pool of 18- to 22-year-olds is substantially younger than normal jury pools. Second, we like to believe Cornell students are well above average in terms of intelligence and education. Finally, most participants were students at the Cornell University School of Hotel Administration, who would undoubtedly be biased toward management when it comes to employment disputes. Even acknowledging these problems, we believe that the experiment has merit. While our 219 students may not be representative of typical pool, they are, in fact, potential jurors.

Study Results

Despite the fact that our sample is clearly skewed in the ways we just described, we found that jury instructions strongly influenced the outcome for our particular sample. The raw numbers show that a disparity did seem to exist between the findings of the different groups. Jurors found for the plaintiff and awarded damages in 22 of the MMWO cases (29%) and 11 of the pretext (P) cases (16%). The mixed motive instruction is more complicated, as the two prongs can lead to the following three different results: (1) no damages; (2) costs and attorneys' fees; or (3) full damages. This group of students awarded either costs and fees or full damages in 34 of the MM cases (45%); that is, they awarded only costs and fees in 28 of the cases (37%), and full damages in six of the cases (8%). A quick look at these raw numbers leads one to believe that employers are better off with a pretext instruction than either of the mixed motive instructions and, depending on the amount of damages and costs and fees, better off with the single-prong mixed motive instruction (MMWO). These raw numbers are not, however, indicative of statistical significance and it is possible that the differences are just a matter of chance. To get a full and clear picture of the connection between jury instructions and the awarding of damages we conducted a statistical analysis of the data by analyzing each set of decisions against each other.

We conducted a statistical analysis of the data by analyzing each set of decisions against each other.

Mixed Motive versus Pretext Decisions

We began by testing whether there are differences in the jury's decision when we compare the first prong of the mixed motive (MM1) against the one-prong pretext instruction (P). Specifically, we wanted to learn whether the number of mixed motive jurors (34) who found that national origin did motivate the employer was significantly different than the number of pretext jurors (11) who found that the employer was liable. As can be seen from

Exhibit 2

Mixed Motive Without (MMWO) versus Pretext (P) Decisions

Not promoted because of national origin or national origin not a motivating factor		GROUP MMWO	P	Total
No	Count	53	57	110
	Expected Count	57.7	52.3	110.0
Yes	Count	22	11	33
	Expected Count	17.3	15.7	33.0
Total	Count	75	68	143
	Expected Count	75.0	68.0	143.0

	Value	Asymp.Sig. (2-sided)
Pearson Chi-Square*	3.478*	.062
w/ Continuity Correction*	2.776	.096
Likelihood Ratio	3.540	.060
Linear-by-Linear Association	3.453	.063

Notes: Pearson Chi-Square and continuity correction are computed only for a 2x2 table; N of valid cases = 143

Exhibit 3

Mixed Motive (MM) versus Mixed Motive Without (MMWO) Decisions

Prong-one question is the only decision for both MM and MMWO		GROUP MM	MMWO	Total
No	Count	42	53	95
	Expected Count	47.8	47.2	95.0
Yes	Count	34	22	56
	Expected Count	28.2	27.8	56.0
Total	Count	76	75	151
	Expected Count	76.0	75.0	151.0

	Value	Asymp.Sig. (2-sided)
Pearson Chi-Square*	13.626*	.050
w/ Continuity Correction*	3.207	.073
Likelihood Ratio	3.861	.049
Linear-by-Linear Association	3.813	.051

Notes: Pearson Chi-Square and continuity correction are computed only for a 2x2 table; N of valid cases = 151; No cells have an expected count less than 5; the minimum expected count is 27.81.

** Our example involves national origin, but it could be any of the other six protected classes: namely, sex, race color, religion, age, or disability.*

the results in Exhibit 1 this differential was highly significant, at the 99-percent level of confidence.[15] In other words whether the mock jury was given a pretext instruction or mixed motive instruction produced a significant difference across the groups as to the finding of the first prong of the mixed motive instruction versus the pretext instruction.

Next, we compared the entire mixed motive instruction—comprising both prong one and prong two (MM2)—against the pretext instruction. Specifically, we wanted to find whether there was a significant difference between the six (of the 76) mixed motive jurors who found that the employer would have acted in the same manner regardless of national origin versus the 11 (out of 68) pretext jurors who found for the company. Using the same statistical tests, we found no significance between the full mixed motive finding and the pretext finding. Thus, before the law changed in 1991 we could argue that whether the judge used a pretext instruction or a mixed motive instruction was irrelevant. The change in the law, however, means that while the ultimate finding is insignificant, the costs and fees component (prong one) is significant.

Mixed Motive Without (MMWO) versus Pretext Decisions (P)

The next question we examined was whether the results of a pretext (P) instruction question differed from the results of the mixed motive instruction without the second prong (MMWO). The raw numbers were as follows: 11 of the jurors (16%) found for the plaintiff in the P cases, and 22 of the jurors (29%) found for the plaintiff the MMWO cases. The results of this analysis are seen in Exhibit 2. As in the last comparison we estimated both the pair-wise comparison chi-square tests and the likelihood ratio and linear-by-linear test to determine the pair-wise and individual group differences. The results show that this differential was found to be marginally significant. Specifically, we found the difference between the MMWO and P group to be significant at the 90-percent level of confidence. This means that it is unlikely that this differential is due to chance, although an outcome by mere chance is possible. Thus, employers faced with a mixed motive instruction and who choose not to have the second prong will, all other things being equal, likely have a more difficult time prevailing under this instruction than they would under the pretext instruction.

Mixed Motive (MM) versus Mixed Motive Without (MMWO)

We also looked at how jurors answered the prong-one question in the two different instructions. Remember, question one is same in both instructions. The only difference is that the MM group faces a second question that is thought to affect the outcome. Here we are assessing the likelihood of a different decision for the two groups simply because the MM group has an option created by the existence of the prong-two question that the MMWO group never sees. MM jurors answered yes (discrimination motivated the employer) in 44 percent of the cases, while MMWO answered yes in 29 percent of the cases. As in the last comparison we estimated both the pair-wise comparison chi-square tests and the likelihood ratio and linear-by-linear test to determine the pair-wise and individual group differences. As can be seen from the results in Exhibit 3, this differential was also found to be marginally significant. Thus, the MM1 and MMWO groups made different decisions with a 90-percent level of confidence. Based on this finding, employers who are faced with low back pay, but high costs and fees should definitely think about limiting the mixed motive instruction to one prong, as suggested by author Baumgarten.

The final question we looked at is whether the MMWO jurors will provide a different final result than the MM jurors once the MM jurors hear both prongs. Based on the earlier data discussion we know that for full liability MMWO found for the plaintiff in 29 percent of the cases and MM2 jurors found for the plaintiff in seven percent of the cases. Once again using the statistical tests, as shown in Exhibit 4, this difference was found to be highly significant. These results now provide a clear indication that the presence of the second prong in the jury's instruction will produce significantly different decisions, compared to an instruction that offers only prong one. The inclusion of the second prong in the jury instructions will likely have a significant and positive impact on the decision from the employer's perspective. Based on this finding, employers faced with a large amount of back pay should include the second prong of the mixed motive instruction.

Conclusion

Our results point strongly to the principle that the legal theories contained in jury instructions matter.

Exhibit 4

Mixed Motive (MM) versus Mixed Motive Without (MMWO) Decisions

Prong-one decision on both and prong-two decision for MM only		GROUP MM	MMWO	Total
No	Count	70	53	123
	Expected Count	61.9	61.1	123.0
Yes	Count	6	22	28
	Expected Count	14.1	13.9	28.0
Total	Count	76	75	151
	Expected Count	76.0	75.0	151.0

	Value	Asymp.Sig. (2-sided)
Pearson Chi-Square*	11.486*	.01
w/ Continuity Correction*	10.111	.01
Likelihood Ratio	12.070	.01
Linear-by-Linear Association	11.410	.01

Notes: Pearson Chi-Square and continuity correction are computed only for a 2x2 table; N of valid cases = 151.

** Our example involves national origin, but it could be any of the other six protected classes: namely, sex, race color, religion, age, or disability.*

Assuming facts that could go either way, employers have a substantially equal chance of prevailing in pretext and mixed motive cases, but there is significant chance that a mixed motive instruction will result in cost and fees being awarded. Employers therefore are better off with a pretext instruction than a mixed motive instruction. If, however, the judge orders a mixed motive instruction, the employer has a difficult choice. The MMWO instruction will more likely yield a complete victory for the plaintiff than will the MM. On the other hand, the chance of the full mixed motive instruction resulting in an award of costs and fees is greater than the likelihood of the one-prong mixed motive instruction, resulting in a complete plaintiff victory. The question that arises is whether the employer should offer the second-prong defense if the judge orders a mixed motive instruction. We believe that the answer depends on the case. If the case is a "fees case" (low liability, but high attorneys' fees),[16] the employer should go with the one-prong MMWO. If liability is high, the employer should stick with the full two-prong mixed motive. Both of these options, however, are worse than pretext instruction.

The CRA of 1991 made the mixed motive instruction much more detrimental to employers. *Costa* made the mixed motive instruction much easier to obtain. As plaintiffs' lawyers become more familiar with the mixed motive instruction they will request it more often. Employers should argue against that approach, but if the judge orders it, employers then need to assess the true costs of their case. If it is a fees case our study suggest employer should use the MMWO. In a case where the potential for substantial back pay is high employers should present the full two-prong mixed motive defense.

About the Authors

David Sherwyn, J.D., is associate professor of law and academic director of the Center for Hospitality Research at the Cornell University School of Hotel Administration. His research focuses primarily on labor and employment law issues relevant to the hospitality industry, specifically, mandatory arbitration of discrimination lawsuits and sexual harassment.

Steven Carvell, Ph.D., is associate dean and an associate professor of finance at the School of Hotel Administration. Among other topics, his research develops models to incorporate real options, risk analysis, and debt capacity into hotel feasibility analysis.

Joseph Baumgarten, J.D., is a partner at the New York office of Proskauer, Rose, a law firm with diversified corporate law practices, where he is a member of the firm's labor and employment practices group and where he focuses on employment discrimination, traditional labor law, arbitration, and other forms of alternative dispute resolution.

Reprinted with permission from Cornell University.
Cornell Hospitality Report, *Vol. 7, No. 1, 2007.*
Cornell Center for Hospitality Research, www.chr.cornell.edu

Endnotes

1 *Desert Palace d/b/a Caesars Palace Hotel & Casino v. Costa,* 123 S. Ct. 2148 (2003).

2 In contrast, Simpson was found liable for wrongful death in a civil case where the standard was preponderance of the evidence.

3 *McDonnell Douglas Corp. v. Green,* 411 U.S. 792, 793 (1973).

4 *Texas Department of Community Affairs v. Burdine,* 450 U.S. 248, 256 (1981).

5 *Price-Waterhouse v. Hopkins,* 490 U.S. 228 (1989).

6 *St. Mary's Honor Center v. Hicks,* 509 U.S. 502 (1993).

7 In many ways *Hicks* makes sense, because employer should be found guilty of discrimination only when the factfinders believe that the employer actually discriminated against the employee. Title VII is not a truth-in-employment act, and there are times when employers, despite their best efforts, may not know why a decision was made.

8 See: Samuel Estreicher, "Saturns for Rickshaws: The Stakes in the Debate over Pre-dispute Employment Arbitration Agreements," *16 Ohio St. J. on Disp. Resol.,* 559 (2001).

9 *Id.*

10 In contrast, the Age Discrimination in Employment Act of 1967 (ADEA) always allowed for jury trials.

11 Subsequent to the 1991 Act, Congress passed the Americans with Disabilities Act, which also allowed for jury trials.

12 David Sherwyn, J. Bruce Tracey, and Zev J. Eigen, "In Defense of Mandatory Arbitration of Employment Disputes: Saving the Baby, Tossing out the Bath Water, and Constructing a New Sink in the Process," *2 U. Pa. J. Lab. & Emp. L. 73.*

13 *Id.*

14 *Supra.*

15 We first ran a Pearson Chi-square test (with and without a continuity correction) to determine whether there are differences in the attribution of motivation across the two instruction sets. We then ran both likelihood ratio and linear-by-linear association tests to determine whether this difference was statistically significant.

16 Sometimes back pay is marginal because the employee found another job, but the litigation costs may be hundreds of thousands of dollars. Other times, both the back pay and the fees are high. It is rare for a case to involve high back pay and low fees.

Sometimes I feel discriminated against, but it does not make me angry. It merely astonishes me. How can any deny themselves the pleasure of my company? It's beyond me.

—Zora Neale Hurston (1903–1960), American folklorist and writer

It is the land that freemen till,

That sober-suited Freedom chose,

The land, where girt with friends or foes

A man may speak the thing he will;

A land of settled government,

A land of just and old renown,

Where Freedom slowly broadens down

From precedent to precedent. . . .

Alfred, Lord Tennyson (1809–1892), "You Ask Me, Why"

Risk Manager as a Grievance Petitioner? Manage Lobbying Risks or Lose

Pamela J. Rypkema, Risk Manager, Gallaudet University

Abstract: While the 501(c)(3) status of many nonprofit organizations (including colleges and universities) limits partisan political activity because of federal tax exemption, it is important for risk managers to know what is permissible institutional involvement in the legislative process and what constitutes lobbying. This article defines lobbying and examines its implications under the standards of the Internal Revenue Service, and offers advice on the management and avoidance of the risks associated with lobbying.

Effective governance depends upon communication between the government and its citizens. To ensure that such necessary communication can occur, the Bill of Rights to the United States Constitution guarantees that:

> Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.[1]

Lobbying is part of our democratic tradition and has become the most effective way to petition the government for funds, action, or new legislation. The term comes from a 19th-century practice at the Willard Hotel, located just around the corner from the White House in Washington, D.C. The Willard was Washington's finest hotel. Many government officials lived at the hotel, and others (including the president) ate there frequently. Petitioners, or their agents, waited to buttonhole government officials as they passed through the hotel's ornate lobby. The term "lobbyist" evolved from a descriptive reference to one of Washington's most important professions.[2]

The term "lobbyist" evolved from a descriptive reference to one of Washington's most important professions.

Recent news accounts have sullied the reputation of lobbying and lobbyists. Consider the convictions of Jack Abramoff (convicted lobbyist), J. Steven Griles (convicted administration official), and Robert Ney (convicted congressman).[3] When the public fails to pay attention, graft and corruption can flourish. Citizen involvement enhances accountability, and nonprofits bring more eyes to the legislative process, genuine concern about the public, and a reasoned debate of the issues.

Are you a "grievance petitioner," or should you be? What are the risks of inserting college or university employees into the governmental decision-making process? What are the risks of failing to do so? This article will help risk managers better understand and manage lobbying risks. It addresses only federal law and only those nonprofit organizations designated tax-exempt under Internal Revenue Code (IRC) 501(c)(3) (most URMIA institutional members).[4] State enforcement of parallel limitations may be more aggressive, and the great differences between state laws are not included in this article. Schools within a church or religious congregation may have special rules, and public institutions are treated differently in some respects than private ones. The article is not intended to be a legal treatise, especially because this topic is becoming a controversial issue for the 110th Congress.[5] URMIA members are advised to consult with legal counsel on questions about this topic.

Understanding Lobbying

In exchange for an exemption from federal taxation, which also allows donors to deduct their contributions to the organization, 501(c)(3) nonprofits agree to limit lobbying activities. Limits to this form of advocacy are designed to maintain the integrity of the tax system and to avoid public subsidies to partisan political activity.[6]

This risk cannot be avoided. People express themselves on and off campus. Current events, and upcoming elections may tempt passionate people to push boundaries further—claiming that the "end justifies the means." Those with opposing views will complain of real or perceived infractions of Internal Revenue Service (IRS) regulations, and both sides, righteously indignant, may debate before the waiting press and prompt the IRS to take action. What cannot be avoided must be managed, so anticipate that some petitions to the government from your campus may constitute lobbying. Good risk management keeps the institution out of trouble.

What is lobbying? Not every communication with the federal government is lobbying. Access to the courts is never lobbying, though supporting or opposing a judicial candidate for Senate confirmation is always lobbying according to the IRS. A truthful response to a congressional subpoena will never violate the law, and participation in the regulatory process is not considered lobbying activity by the IRS.[7] The risk exposure depends upon which branch of government receives the advocacy and why.

Limitations to a 501(c)(3) organization's petition to the government fall within two categories: "political" (campaigning and electioneering) and "legislative" (proposing, supporting, and opposing legislation—including appropriations).

Some petitions to the government from your campus may constitute lobbying.

Campaigning for a Candidate: Prohibited Political Activity

Political campaign activities are absolutely prohibited.[8] There is no *de minimus* exemption, nor is there a defense based on ignorance of the law. Any distribution of statements (oral or written) on behalf of, or in opposition to, a candidate and all campaign contributions are prohibited.

A school employee may promote a candidate, even work on a campaign, if "off-the-clock" when the employee is serving in a personal capacity. However, no 501(c)(3) employer supplies or resources can be used in the endeavor. Designated institutional spokespersons must also be very careful. Defending "personal" speech or activity becomes increasingly difficult when the personal views can get confused with institutional views.

Nonprofits can provide fair and balanced facts about all candidates, or sponsor a fair and neutral forum for all qualified candidates with an impartial moderator and a broad range of topics. Fundraising for any candidate is prohibited. Unbiased and nonpartisan summaries of voting records and position statements are not considered campaign activity. It is the bias toward a particular candidate and partisanship that makes these educational practices illegal.[9]

Colleges and universities cannot support or oppose a person's bid for office. The IRS recently strengthened its guidance with a revenue ruling to help nonprofits stay within legal requirements when involving candidates, educating and registering voters, and organizing vote drives.[10] Note that not all contact with an elected official is considered campaigning just because the person is running for re-election. It may be acceptable to invite the official to a ribbon-cutting ceremony, an event to receive or give an honorary award or degree, or a speaking engagement at a government class on campus or an educational program. When in doubt, consult with an attorney.

Influencing Legislation: Acceptable Within Limits

The IRS permits lobbying as long as this activity is not a "substantial" part of the 501(c)(3)'s operations. A petition to any legislative branch of government (local, state, or federal) is considered lobbying, as is communication with presidential officials who participate in the formulation of legislation. Congress often expresses broad goals in a statute, which is then implemented by an administrative agency, but participation in administrative rulemaking is not considered lobbying (though the advocacy role is much the same). Expenditures for lobbying, to exert influence over actual legislation, are limited by the IRS.

Through the Lobbying Disclosure Act (LDA), discussed below, Congress also requires a registration for lobbyists so that interested individuals can easily discover who is lobbying for what interests. This adds an element of transparency to the process. The lobbying definition extends to a broader scope of officials than the IRS provisions, but is limited to federal contacts. State laws

may require disclosure of state-level lobbying. The LDA requires disclosure of contacts, not expenditures, and a general summary of each is below.

1. IRS/Treasury Regulations

Lobbying is a form of advocacy, but not every advocated opinion or position constitutes lobbying. Treasury regulation excludes:[11]

- ***Nonpartisan research and study:*** Data collected from unbiased questionnaires or surveys, and evaluation of data, is permitted even if a position is expressed as long as people can form an independent opinion or conclusion about the issue. There can be no call to action, or encouragement for people to contact their legislators.
- ***Government-requested technical advice:*** Reports or testimony offered on a nonpolitical, bipartisan basis at the government's request are not considered lobbying.
- ***Self-defense:*** If the institution's existence, powers, duties, or tax-exempt status is in jeopardy, communications with legislators or the general public is not considered lobbying.
- ***General public interest:*** The institution is permitted to consider, and take a position on, broad social or economic issues if it does not refer to or encourage particular action with respect to pending legislation. Active citizenship is not considered lobbying.

The only complete prohibition when influencing legislation is that you cannot use federal money from grants or contracts, in whole or in part, to attempt to lobby or influence legislation to receive the award.[12] As for other money, there is flexibility for truthful advocacy unless it devotes a substantial amount of its activities towards lobbying.

"Substantial" is subject to interpretation, and even limited lobbying by an influential or prestigious institution may be considered substantial by the IRS. The IRS allows a nonprofit to elect a specific definition under IRC 501(h),[13] in which "substantial" is determined by the level of expenditure (which is broadly defined) on lobbying activities. Schools should opt for the certain standard. Overall, election under 501(h) simplifies requirements (described in IRS Form 5768), offers a clearer measure of "substantial," makes expenditure tracking and recordkeeping easier, and gives the IRS more favorable flexibility when sanctioning a rule violation.[14]

For instance, a volunteer's efforts are not lobbying unless he or she is reimbursed for expenses or uses nonprofit resources and supplies (office, computer, server, paper, phone, etc.). It is the expenditure of money (directly or indirectly) that transforms the free speech into lobbying activity. For any communication that combines both educational speech and legislative advocacy (perhaps a newsletter with articles on varying topics), the college or university must allocate expenditures between purposes. However, the organization sets the rules. The IRS permits great flexibility with allocation if the school articulates and adopts a reasonable method in good faith, and if the allocation is fair. To continue the example, a newsletter has 10 articles, but only one considered to be lobbying. Allocating 10 percent of the newsletter's cost for lobbying expenditures might be appropriate.

Participation in administrative rulemaking is not considered lobbying.

Expenditure thresholds differ between two categories: grassroots/indirect lobbying and direct lobbying. In the former category, petitioners urge the general public to contact legislators. This typically involves education about the issue and advocacy of a social or economic position (perhaps through direct mail or an advertising campaign), but it also involves a "call to action" that defines the communication as lobbying. Grassroots lobbying has a lower expenditure cap than direct lobbying.

In the latter category—direct lobbying—petitioners communicate directly with legislators. This contact may include personal meetings, letters or postcards, faxes, e-mails, or other forms of communication. If citizens serve as legislators by voting directly on an initiative or referendum, then trying to influence public opinion is considered "direct" lobbying for expenditure thresholds.[15]

What is Permissible?

In the government arena, the good news is the analysis rests upon facts and circumstances that the college or university can control.

The bad news is the analysis also rests upon facts and circumstances subject to reinterpretation with the benefit of hindsight. Consider the following examples with your school's lawyer:

- President Pam writes a feature article for an alumni magazine called *My View*. In this edition of the magazine, she endorses John Doe, who is running for re-election to Congress from the 62nd District of Virginia. John is an alumnus and personal friend. Pam offers to pay the entire publication expenses for this edition of the magazine from her personal bank account "to prevent trouble with the IRS."

  While announcing someone's activities in an alumni magazine is not campaign activity, endorsing a candidate is. A personal connection, or paying from a personal account, is not likely to placate the IRS. Pam is campaigning, which is prohibited. She does have First Amendment rights to speak, but not in this regular forum which is offered to her as president and spokesperson of the institution. Perhaps if she chose another forum and specified that her personal—not institutional—opinions were expressed, her endorsement might not affect the institution. Consider, though, the range of non-lobby risks that this public opinion may create for the school.
- Director Dan heads the university press at the same campus, knows John Doe, but thinks Congressman Doe is a disaster for the country. Dan personally pays for a full-page ad in the local community paper, which is steeply discounted for prime space because of the relationship between the two publishers. The ad accurately describes Doe's voting pattern, but some language accuses the congressman of hatred for the press and open debate. Payment is made from Dan's personal account, and the ad clearly states the views to be Dan's personal opinion. Past performance, without reference to the upcoming election, is appropriate for public debate. But Dan used his nonprofit contacts for this personal endeavor, and use of this "nonprofit resource" may trouble the IRS. The ad is also likely to be a divisive distraction to the campus community.
- International Ingrid is the study abroad coordinator. She went to school with John Doe, but does not follow politics. The Council for a Limited Press (CLP) wrote an excellent article for journalism students who study abroad. Ingrid links to the CLP website, which is subsequently changed to endorse Congressman Doe for re-election. This endorsement may be considered "campaigning" by Ingrid for John Doe and a problem for the 501(c)(3).
- Adam Alumni Director runs against John Doe for the congressional seat. He refrains from campaigning at work, though he always wears a button supporting his candidacy. Adam uses his school laptop to draft speeches, manage mailing lists (copied from the school alumni list), and to coordinate his work and campaign calendars. But he only works on his campaign at home. Occasional fundraising calls are made from his office, but only on breaks and with no toll or long distance charges to the campus. Still, Adam has created trouble for himself and the school. The button is on his person, not attached to campus property, but may be the only way he complies with the law. Use of his office, phones, computer, university-owned software, and any other nonprofit resources is illegal. Mailing lists can be sold at fair market value, but free distribution is, in effect, an illegal campaign contribution even if the same contribution is given to all candidates.
- Clarissa Clerk holds Adam in high esteem. She wants to contribute to his campaign, but she forgot her checkbook and ATM card. Clarissa "borrows" $50 from petty cash and plans to replace the money the next day. In addition to theft, depending upon the circumstances, she possibly has caused the institution to violate the federal IRS prohibition—even if she eventually returns the money.
- Dr. Vocal Volunteer is a member of the political science faculty, and he supports Adam's bid for office. Dr. Volunteer's office is plastered with signs, bumper stickers, and other campaign paraphernalia. He openly opposes John Doe's vote on war funding at department meetings and whenever he sees people in the hallway. Dr. Volunteer has written countless articles and letters to the editor about the war vote, and he encourages his classes (and anyone within earshot) to do the same. However, he is probably not campaigning. Paraphernalia is in a personal space and obtained with personal funds. Discussion with his colleagues during work hours is likely to be insufficient grassroots outreach, and his activism tools fall squarely within the content and

While announcing someone's activities in an alumni magazine is not campaign activity, endorsing a candidate is.

purpose of his courses. However, from a non-lobbying perspective, his excessive advocacy might cause students with opposing views to question the fairness of Dr. Volunteer's treatment of them. Responsibility accompanies academic freedom, and his intensity may cause other problems that need to be addressed.[16]

- Dr. Paula Freedom is asked to testify as an expert before the House Judiciary Committee about a pending bill supported by CLP (H.R.123), sponsored by Representative Jane Roe, from the 99th District of Montana. Dr. Freedom will incur expenses to prepare the testimony and travel to Washington, D.C., but these probably are not lobbying expenses. Dr. Freedom is responding to a government request, possibly by subpoena. As discussed in the next section, her activities are also not likely to make her a lobbyist under the Lobbying Disclosure Act.

2. Lobbying Disclosure Act

First Amendment protections make direct regulation of professional lobbyists difficult. In 1995, Congress enacted the Lobbying Disclosure Act[17] to increase transparency to contacts with legislators (grassroots is not included) through a registration and reporting system. If at least one employee spends 20 percent of his or her time on lobbying activities, and if the organization spends at least $24,500 every six months on lobbying activities, the college or university comes under the Act.

Lobbying is defined by contacts, not expenditures, and it includes any oral or written contacts with: (1) a member of Congress (House or Senate) and his or her staff, and (2) senior-level presidential officials (regardless of participation in the legislative process). Contacts with state or local officials do not need to be disclosed. Contact disclosure is required if made to influence: (1) federal legislation; (2) federal rules, executive orders, or policy positions; (3) negotiation, award, or administration of a federal program, contract, grant, loan, or license; or (4) nomination subject to Senate confirmation.

Once the LDA applies, disclosure of lobbying contacts by non-lobbyists may be required. For instance, College President visits Capitol Hill. Preparing for the discussions and travel to the Hill involve costs. Disclosure may not be required if the visit was educational or at the government's request (for instance, to speak to a large group, or testify before a committee or subcommittee), or if communication is required by grant or federal contract. Disclosure is probably required if he comes under the Act and if visits were to discuss an appropriations bill earmarking funds for the institution.[18] For those who socialize with Hill staff, might brief discussions about legislation with a Senate staffer during a child's soccer game count as a "contact"?

Many had criticized the Act's generosity for gifts and travel and omission of entertainment and fundraising activities. In other words, there was full disclosure except for the circumstances that offer great temptation for corruption. New ethics rules and changes to the LDA ban gifts to members and their staff members, put limits on entertainment, impose new rules on employing/retaining lobbyists, and change the disclosure reporting format and frequency.[19] Talk to your institution's legal counsel about any gifts, travel or entertainment expenses, or fundraising activities for a government official or about any close relationships with legislative staff. Those free tickets to the championship basketball game for a congressional staffer may not be so innocuous, nor might the expensive dinner at the trendy nightspot or a ride offered to a senator in the university plane.

Assessing the Risk

The legal risk of noncompliance is high and the potential consequences catastrophic. The IRS evaluated a small number of nonprofit organizations (all 501(c)(3), but not all schools) after the 2004 election. Its conclusions are startling: 75 percent of the organizations were engaged in some level of prohibited political activity. The IRS has many ways to punish campaigning and excessive lobbying, and revocation of an institution's nonprofit status is the most devastating.[20]

Expenditures for lawyers and media consultants during the investigation may pale in comparison to any resulting lost (or delayed) donations to the institution. As a small consolation, these self-preservation contacts may no longer constitute lobbying. But beyond donations, the blow to the institution's reputation for its alleged failure to manage its affairs within the confines of the law may result in decreased enrollments and an inability to hire the best and brightest faculty for years to come. Battling the IRS is also likely to invite further scrutiny by other

interested parties: media, other regulators, collaborating institutions, vendors, etc. All of this distracts from the university's central mission: educating students and conducting research.

Colleges and universities are also uniquely at risk due to the degree of decentralization, academic freedom traditions, and the perceived innocuousness of the conduct by those not familiar with the complex rules. Many legislative issues also affect a faculty member's profession, scope of research, and ability to fulfill his or her service requirements for tenure evaluation. For instance, it would be nonsense for the chair of the social work department to refrain from weighing in on licensure of social workers and practicum requirements for his students. However, it would be dangerous for him to extract a pledge from a candidate to support a certain position on social work issues (implied endorsement) and then to encourage his students to support the candidate.

Enormous opportunity costs exist for not speaking up out of ignorance or fear—institutions can be forced to operate in the legal environment created in our absence. Imagine a world where nonprofits are silent and no one speaks for intangible interests unless it is profitable for business to do so. Does this reduce the value of our missions to a mere cost/benefit analysis after calculating the rate of return necessary on the tuition expenditure? Does an educated populace offer other benefits to society? Silence deprives the government of a more balanced perspective—including the value of intangible benefits that are difficult to measure in the commercial marketplace. It is important that we know what is allowable under the law.

Silence may waste time and money, as well. Congress, and the agencies trying to implement public policy with practicality and without undue burden, recognize that political discourse is more effective with expert participation, and that decisions are better when representatives of regulated industries or professions speak up. As risk managers, we know it is always better to do something right the first time rather than fix it later. Campus education empowers those who are not typically advocates (but who have a valuable perspective), facilitates constitutionally encouraged comment, and helps campus petitioners stay within legal limits.

To demonstrate, consider a regulatory example (which is not considered lobbying) of a regulation of hazardous substances. The business lobby supported the regulation as better than the alternatives. Businesses used only a few different substances, but in great volumes, so compliance was easy. But a local college had a laboratory that contained small quantities of a large number of hazardous substances. Compliance for the college would have been costly and time consuming given the diversity of substances. The chair of the chemistry department viewed speaking up as beyond her job description and talents, and she was too busy to figure out the process. Everyone loses if she does not participate in the initial rulemaking.

Decisions are better when representatives of regulated industries or professions speak up.

Involvement with government decision-making can also improve our institutions. Getting involved exerts some control over the legal environment—blocking legislation and regulation that does not make sense, and refining legislative and regulatory language so that compliance is practical and realistic. It facilitates compliance and prevents legal trouble. It can bring campus departments together and create opportunities for teamwork and collaboration.

Managing "Petition" Risks, and Including Risk Management in the Process

How does an institution manage its government petitions and involve itself in governmental decision-making? Risk managers are a valuable resource as the college or university manages these petition risks, but as a member of a much larger team. Colleges and universities should keep the following strategies in mind.

Centralize the Management of Lobbying Risk

Trustees delegate general operations and spokesperson duties to the president—this is where lobbying risks should be managed and will receive greatest respect from the campus community. It is also easy to remember a single office for any questions or approvals. If the policies

are unclear, people may go ahead, speak on behalf of the institution, rationalize that it is easier to ask for forgiveness than to obtain permission, and potentially jeopardize the school's tax-exempt status. Clear policies minimize noncompliance, but if an infraction still occurs, it is more likely to be an isolated event (considered by the IRS when determining sanctions).

The president's office, however, is well-advised not to manage and control these risks alone. A government relations committee can quickly tap a diverse range of expertise from across campus to maintain campus policies and procedures, field questions, and investigate complaints. Committee members can keep a watchful eye for legislative developments in professional literature that potentially affect the school. They can decide to participate in governmental deliberations, or plan corrective action to comply with evolving requirements. This can even be as informal as an internal listserv.

One person on the committee can serve as an expert on legislative process, and can track bills that the school cares about, but all committee members should know:

- The names of the institution's geographic representation—both senators and representatives on the federal level, and all representatives at the state level.
- The names of the institution's jurisdictional representation—for higher education, at the federal level, target all members and key staff of the Labor, Health and Human Services, and Education committees.
- The names of any members with a special interest in the school—a caucus along race (the Black Caucus) or gender (the Women's Caucus) or geography (the State or Rural Caucus); alumni from your institution; congressional members who have family members currently at your institution; and anyone already sympathetic to, or who already advocates for, your cause.
- The basic process for making legislation, and the points within the process where lobbying might be useful (where you can block or modify proposed legislation).
- Your institution's philosophy and policies on government affairs.
- Issues appropriately resolved through governmental action. The government is not the source of all remedy, and lobbying on the wrong issue will just waste your time and money. Technology, staff training or reassignment, or another strategy may be a better solution to the problem.
- General services that are available from lobby firms, to ensure effective retention of outside professionals if appropriate.

Team involvement can prevent good, but uninformed, intentions from creating a poorly written law.

Include the Campus Risk Manager

The campus risk manager is a valuable resource to the committee. He or she may become aware of troubling allegations while working on campus, through observation or a complaint. Allegations of campaigning or acceptable lobbying may be mentioned during venting, or as an aside. Risk management spans the campus, and the risk manager is the centralized office that works with every department and coordinates these risk management efforts. The risk manager can be the ears and eyes of the committee.

Beyond appropriations, many legislative issues have operational implications of which the president may not be aware or as expert. For example, there has been discussion on Capitol Hill about creating a parallel reporting statute to the Clery Act for fire safety.[21] Risk managers bring a practical, operational perspective to proposed language and can help develop a more reasoned position. Team involvement can prevent good, but uninformed, intentions from creating a poorly written law (one that then will need to be thrown out by the courts, after much legal expense). Practical citizen input results in better legislative decision-making and a better use of public resources, and this input gives risk managers a chance to practice what they preach by addressing a situation when it is small and manageable rather than waiting for a crisis.

Typically, a campus risk manager can add insight and resources on issues such as building sprinkler requirements, hazardous waste disposal, construction,

laboratory safety, industrial hygiene, animal research, security, emergency preparedness, statutory indemnification, immunity statutes, dispute resolution, intellectual property risks, study abroad, student internships and practica, athletic safety, worker safety standards, driver qualification requirements, and employment practices.

Insurance itself is an important legislative issue. Coastal schools understand the importance of insurance to continued viability, but private insurance still might need support from the federal government after a disaster. A lack of insurance for terrorism after 9/11 required congressional help.[22] A movement to nationalize regulation of insurance is also underway, with both benefits and drawbacks to the commercial insurance purchaser. When insurers fail to honor promises, or when a whole-scale jurisdictional change is proposed, legislators often hear from private homeowners but less from commercial buyers. However, purchasing decisions, recovery expectations, and claim complexity differ significantly between the two types of insurance purchasers. Legislators do not always understand insurance products, so risk managers need to keep up, speak up, and protect the institution's interests.

Education removes paralysis from fear and empowers a risk manager to respond to regulatory developments. Although not lobbying, risk managers who do not know the distinction may shy away from shaping regulatory issues that sometimes have a greater impact on the college or university than legislative enactments. Committee involvement provides such an education and makes it easier to speak up and to be effective.[23]

Existing resources are more easily expanded than new programs created from scratch. Risk assessment, legal compliance, training, and education tools are already in the risk management toolbox. Can these tools be expanded to identify government interaction risks? Many risk management offices are equipped with systems to collect, organize, track, and report on extensive data for insurance purposes. Perhaps another use for these systems is to track lobbying expenditures and avoid exceeding the IRS limits—a process similar to tracking insurance deductible expenses. Why reinvent the wheel?

Finally, the risk manager has developed outsourcing expertise from retaining brokers, lawyers, safety consultants, contract drivers, or other vendors or professionals. A request for proposal (RFP) tool may be helpful when selecting a professional lobby firm, too. Documenting processes already exist to check qualifications and references, negotiate the contract, and arrange for payment after satisfactory completion of the work. Again, why reinvent the wheel?

Educational efforts increase compliance, and such efforts also demonstrate your due diligence.

Educate: What Schools Do Best

On this issue, everybody on campus must comply so prevention must be campus-wide. Education is one tool that colleges and universities already deploy. Institutional policies can serve as notice, but also resource documents. Clearly prohibit what is prohibited under the law, and disclaim any institutional responsibility for illegal speech or conduct. Create a workable process to approve and track lobbying expenditures. Assign the task of monitoring expenditures to a particular position or department. Then tailor guidance documents for different campus constituencies. A general written summary may be sufficient for professional and other staff, but offer more extensive training to department chairs, budget directors, or other supervisory employees. Also consider how to involve and equip the institution's board of regents or trustees. Ultimately, conservation of the institution's resources is the board's responsibility. Consider other awareness programs and e-mail reminders (such as when passions are high before an upcoming election). Expand Constitution Day[24] to educate faculty and staff. Educational efforts increase compliance, and such efforts also demonstrate your due diligence.

Outsource Where Appropriate

It is likely that part of this risk will be outsourced or transferred to others. This is not an easy process, and consideration of the issues will take quite a bit of the government relations committee's time. Outsourcing also

does not mean there is no role for the institution and its employees. To the contrary, any good lobby firm will consider ways to effectively use campus resources in the advocacy process: testifying, personal visits to congressional offices, letter-writing campaigns, strategically placed letters to the editor, press conferences or releases, etc. In essence, you are outsourcing the leadership of lobbying activities to a firm with greater expertise and resources.

1. To A Separate Campus Entity

If you anticipate extensive lobbying, it may be advisable to transfer the entire risk to an affiliated organization, perhaps a 501(c)(4) or 527 nonprofit organization. Although these entities are nonprofit, people cannot deduct from their taxes any donations to these entities.

The institution can control the lobby activities, but it must respect the arms-length relationship between the school and the separate entity. Any shared personnel, facilities, or resources must be allocated between the school and separate entity, and the separate entity must pay its fair share.[25] Full analysis of this risk management strategy requires the assistance of an experienced tax attorney.

2. To Professional Associations

Most professional staff, and almost all faculty, belong to a professional association or trade group. Many are "nonprofit" under IRC 501(c)(6), which means that donations are not tax-deductible but that resources (human and financial) can be aggregated to lobby. Legislators also like to see existing consensus of insurance or higher education professionals on an issue.

Professional associations tend to involve members in the lobbying effort, and these members are also employees of your institution. The school's policy should address when the employee is an agent working on behalf of the outside association, and when the employee acts on behalf of the institution. Reimbursement of expenditures should come from the sponsoring entity for these lobbying activities, and communication should also appropriately identify the entity (for example, use association letterhead rather than institutional letterhead for association business).

3. To a Professional Lobbying Firm

Federal lobbyists do not have licenses or permits, and there is a wide variety of skill and experience that each one brings to the profession. First, define your long- and short-term goals and scope of work. To illustrate, the horror at Virginia Tech prompted a quick legislative proposal to amend the Family Educational Rights and Privacy Act (FERPA) and to prevent future shootings. However, language proposed would achieve the opposite of Congress' intent. A short-term goal may be a public relations campaign to block the bill. A long-term plan may be to set up a judicial challenge if the bill is enacted. For the former, you may need a PR firm that does lobbying and governmental work. For the latter, you may need a law firm that has a government practice.

Professional firms can offer a variety of services, and what you buy depends upon your goals.

Professional firms can offer a variety of services, and what you buy depends upon your goals. You get more bang for your lobbying buck if you have a clear idea what you need before retaining a firm. The university's options may include a firm to:

- Give access to influential members of key committees (such as Appropriations) and open doors. Typically, these firms have hired people with direct access to key Capitol Hill offices.
- Offer specialized expertise to frame the public issue or governmental question and then advocate for your institution's position within this new framework.
- Keep you abreast of developments on Capitol Hill, perhaps offering a newspaper clipping service, inviting personnel to speak to campus leaders and field questions, and enlisting clerical support to manage direct mail.
- Manage grassroots campaigns— one familiar with buying television and other media time, organizing direct mail, writing and distributing newsletter alerts and advertising content, maintaining databases and grassroots networks, and conducting phone bank operations.
- Provide a network from which to build and manage coalitions around a public issue for greater lobbying impact.

- Keep the school in compliance with the lobbying laws.

Second, define what you want in the lobbying team. Good interpersonal skills are a must: integrity, honesty, ability to patiently listen, diplomacy, creativity, thoughtful thinking, persuasive advocacy, and responsiveness to the client (you). Consider whether you want the firm to have experience with other colleges and universities.

Then the team must develop a suitable strategy and have the resources to devote to achieving the desired goals. On any given issue, is it better to lobby Congress or the executive branch (President and cabinet)? Will a mix of direct and grassroots lobbying be effective, or should the school go with either direct or grassroots? What is the plan to capture the interest of particular senators and representatives—those chosen for party and influence, or because they can influence a regulatory agency? Is it equally important to cultivate support among enthusiastic staffers in the congressional offices? Is a bipartisan approach better than a partisan one? Regardless of strategy, make sure the firm keeps you in the loop as it represents your interests.

Third, negotiate an engagement letter with the firm. The letter will describe the scope of work, but also how and when you will compensate the firm. Contingency payments are prohibited in many states, though the federal law is not clear. Think through whether an external incentive is necessary to obtain effective services from the firm.

Finally, be generous with "thank-yous" and follow-up correspondence. Members of Congress and their staff hear complaints 99 percent of the time. Notes of appreciation are time consuming, but you will distinguish your school from the complaining crowd if you write them. The outside lobbying firm may offer clerical help for this purpose.[26]

Be Proactive, not Just Reactive

Lobbying should not just be blocking or reshaping flawed bills. This is analogous to limiting visits to the doctor when someone is sick. After appropriate consultation with legal counsel, invite members or staff from Capitol Hill to campus events. Share helpful nonpartisan studies or success stories from the school. Send press releases that may be of interest to his or her constituents. For a particular bill, help draft a bank of questions for an upcoming hearing. If you are seeking legislative help, offer more than one possible solution that might fix it. Give your congressional delegation positive information and constructive solutions that can be used to serve you well.

Give your congressional delegation positive information and constructive solutions that can be used to serve you well.

Developing Better Institutional Risk Management

Our democracy requires citizen input, and input from your campus gets more diligence from legislators, better value from invested time and money, some control over the legal environment, and new opportunity for campus collaboration. Failure to manage the risks may result in loss of the school's tax-exempt status.

Risk managers also may find it easier to identify and manage more routine risks because petition-related risks often dovetail into risks of daily concern. Early involvement allows time to shape proposed changes and to implement compliance plans when the legal environment changes. It potentially increases the interaction with various campus constituencies, and the more known about campus activities and pending developments, the better position from which to evaluate the adequacy of the institution's insurance safety net. If a department must comply with new regulations, the risk manager can also help spot and manage other risks created during the changes. Any success stories or positive anecdotes collected can be shared with insurers and used in claim situations.

However, to be a valuable resource, risk managers cannot be tethered to just those risks covered by insurance (which are not likely to be lobby-related risks), nor be passive recipients of governmental news. Risk managers must actively keep abreast of legislative and regulatory issues and speak up when appropriate. They must care about all the risks of the educational enterprise, and be part of the team to make both the institution and the United States of America the best that they can be.

About the Author

Pamela J. Rypkema is the risk manager at Gallaudet University in Washington, D.C. She expresses great appreciation to her colleagues who contributed to this article, including: Gary Andreas, Vice Chairman of Public Policy and Research (Dutko Worldwide); Caleb Burns, Attorney (Wiley Rein LLP); Ada Meloy, General Counsel (American Council on Education); Tom Rudin, Senior Vice President for Advocacy, Government Relations, and Development (College Board); Ben Wallerstein, Vice President and Counsel (Dutko Worldwide); and Joel Wood, Senior Vice President, Government Affairs (The Council of Insurance Agents & Brokers).

Endnotes

1 United States Constitution, Amendment I.

2 J. Baran, "Can I Lobby You?," *Washington Post,* January 8, 2006; History of the Lobbying Disclosure Act (Public Citizen 7/23/07).

3 See Wikipedia online at www.wikipedia.org/wiki/Jack_Abramoff; www.wikipedia.org/wiki/J.Steven_Griles; www.wikipedia.org/wiki/Bob_Ney.

4 See www.npaction.org/article/articleview/48/1/227 for a list of nonprofit classifications.

5 See S.1642 (Kennedy-Coburn Amendment to the Higher Education Act of 1965 Reauthorization, which restates the IRS campaigning and lobbying regulations). The issue remains political. In addition to the institution's lawyer, consult with any employed or retained lobbyists for interpretation and guidance as legal requirements evolve. Information concerning bills referred to in this article can be obtained from www.house.gov or www.senate.gov.

6 Congress confirmed the right of nonprofit organizations to undertake legislative advocacy, P. L. 94-455 (1976), and reaffirmed the right in 1987 when amending the Act. Regulatory jurisdiction is delegated to the IRS, and the regulatory framework was completed in 1990. See 26 U.S.C. Section 501(c)(3); *Hernandez v. Commissioner,* 490 U.S. 680, 699–700 (1989) (501c3 balance is least restrictive way to accomplish compelling interest of preserving integrity of tax system); *Regan v. Taxpayers With Representation of Washington,* 461 U.S. 540, 546 (1983) (Congress not required by First Amendment to subsidize lobbying); *United States v. Harriss,* 347 U.S. 612 (1954) (restrictions do not violate freedoms guaranteed by the First Amendment—freedom to speak, publish and petition the government); IRS Publication 557; IRS Form 5768.

7 Congress delegates rulemaking authority to administrative agencies. These agencies depend on comments from those regulated and solicit these comments by holding hearings (formal rulemaking), accepting comments by letter, fax, or e-mail (informal rulemaking), or creating a focus group of sorts to create a workable regulation (negotiated rulemaking). See 5 U.S.C. Sections 551, *et seq*. (Administrative Procedures Act).

8 See The Revenue Act of 1954, P. L. 83-91; 26 U.S.C. Section 1 *et seq.;* IRS Publication 557. Public employees also may be barred from political activity under federal law. www.osc.gov/ha_fed.htm.

9 IRS Rev. Rule 86-95, 1986-2 C.B. 73, IRC Section 501(c)(3); IRS Publication 557. The United States Supreme Court recently struck down part of a campaign finance law because it interfered with free speech. In *Wisconsin Right to Life v. The Federal Election Commission,* Docket 04-1581 January 2006 (www.supremecourtus.gov/opinions), Chief Justice Roberts said that: "[w]here the First Amendment is implicated, the tie goes to the speaker, not the censor." Although this decision may cause re-evaluation of campaign speech, it is unlikely to grant permission for nonprofits to speak. The decision looked at FEC, not IRS, rules, and the two regulatory frameworks are vastly different. The recently proposed amendment to S.1642, referenced in endnote 6, demonstrates congressional support for the existing IRS regulatory position.

10 IRS Rev. Rule 2007-41, 2007-25 I.R.B. (June 18, 2007).

11 Treasury Regulations 53.4945-2(d). In addition, each federal agency may have special regulations aimed at controlling lobbying with the agency.

12 31 U.S.C. Section 1352 (Byrd Amendment); 34 C.F.R. Part 82. See OMB Circular A-21; A-122 (relocated to 2 C.F.R Section 230); A-133.

13 Tax-exempt organizations under 501(c)(3) may elect safe-harbor rules to govern lobbying expenditures under Section 501(h), which gives a specific formula for determining permissible lobbying activities and allows the organization to rely on the limitations in Treasury Regulation 56.4911 *et seq*.

14 A nonprofit organization in the IRC 501(h) safe harbor may benefit under the Lobbying Disclosure Act too. Entities that elect the 501(h) definition of "substantial" do not need to keep two sets of books or establish two compliance procedures, but instead can opt for the IRS definition. Section 15(a) of the LDA permits an organization in the safe harbor to attach a copy of its IRS Form 990 to the required lobbying disclosure report. Compliance under the vague "substantial" standard imposes a double reporting process: one to the IRS and one to the secretary of the U.S. Senate (sopr.senate.gov) and the clerk of the House of Representatives (clerk.house.gov). See Guide to the Lobbying Disclosure Act at lobbyingdisclusre.house.gov/lda_guide.html; J. Tenenbaum, "Top Ten Myths about 501(c)(3) Lobbying and Political Activity," *ASAE* (May 2002).

15 *The Nonprofit Lobbying Guide, Second Edition,* Independent Sector. See www.independent sector.org/programs/gr/lobbyguide.html.

16 See *Garcetti v. Ceballos,* 126 S.Ct. 1951 (2006) (the First Amendment does not insulate a public employee from discipline for official statements); *Pomona College v. Superior Court,* 53 Cal. Rptr.2d 662 (Cal. App. 1996) (tenured teacher is not immune from termination; discharge is appropriate if personal conduct substantially impairs the person's fulfillment of his or her responsibilities).

17 The Act applies to both for-profit and nonprofit organizations. See P. L. 104-65 (Dec. 19, 1995); 2 U.S.C. Section 1601; clerkweb.house.gov/lrc/pd/lobby/lobby.htm; www.senate.gov/legislative/common/briefing/lobby_disc_briefing.htm. Forms are available from the Senate Office of Public Records and the House Legislative Resource Center.

18 Non-lobby contacts may count under Section 3(10) of the Act. Lobbying includes planning and background work necessary for the contact, as well as coordination with the efforts of others. See J. Tenenbaum, "Lobbying Disclosure Act of 1995: A Summary and Overview for Associations," *ASAE* (June 2002).

19 See 2 U.S.C. section 1601; www.independentsector.org/programs/gr/lobbyreform.html; *Election Law News* (February 2, 2007) at wileyrein.com.

20 See IRS Rev. Rule 2007-41, 2007-25 I.R.B. (June 18, 2007); IR-2006-36 (news release) FS-2006-17 (fact sheet) at www.irs.gov/newsroom; *Branch*

Ministries v. Rossotti, Order No. 995097A (D.D.C. 2000); IRS Publication 557.

[21] Congress is wading into more traditional risk management areas. Legislation was proposed after the Seton Hall fire in 2000 ("Campus Fire Safety Right-to-Know," H.R. 2637, a Senate version passed on July 24, 2007). On June 20, 2007 the Committee on Health, Education, Labor, and Pensions passed a proposal to impose on colleges and universities 100 new reporting requirements concerning a range of operational issues.

[22] The Terrorism Risk Insurance Act of 2002, recently extended (signed five days before the Act expired), provides a temporary federal terrorism insurance program. See www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/pdf/hr3210.pdf. Other issues include: insurance regulatory reform (H.R. 1065/S.929); flood insurance reform (H.R. 920); and technical requirements to block file sharing (H.R. 3746). To track insurance legislation, risk managers might want to use the resources of The National Conference of Insurance Legislators (www.ncoil.org), and the Risk and Insurance Management Society, Inc. (www.rims.org).

[23] On a regulatory front, the U.S. Department of Homeland Security may alter federal hazardous chemical regulation because proposed rules would be too burdensome for colleges and universities. L. Smith, "Federal Panel Will Discuss Modifying Chemical-Security Regulations to Suit College Needs," *Chronicle of Higher Education* (July 25, 2007). Speaking up saves time and money.

[24] P. L. 108-447, Consolidated Appropriations Act of 2005, requires any institution receiving federal funds to hold an educational program for students on September 17th each year about the U.S. Constitution. Ongoing compliance efforts can easily be expanded to reach a faculty and staff audience, too.

[25] See *Regan v. Taxpayers With Representation of Washington,* 461 U.S. 540(1983); and the list of various nonprofit organizations from the NP Action website in endnote 4. For general information, see the Campus Legal Information Clearinghouse at Catholic University, http://counsel.cua.edu.

[26] Excellent resources include:

- American Council on Education (www.acenet.edu)
- American Society of Association Executives (www.asaecenter.org)
- Center for Lobbying in the Public Interest (www.clpi.org)
- Independent Sector (www.independentsector.org)
- League of Women Voters (www.lwv.org)
- NP Action (www.npaction.org)
- National Council on Nonprofit Associations (www.ncna.org)
- Public Citizen (lobbyinginfo.org)

Remember, man, 'The universal cause
Acts not by partial, but by gen'ral laws;'
And makes what happiness we justly call
Subsist not in the good of one, but all.

—Alexander Pope (1688–1744), "An Essay on Man: Of the Nature and State of Man with Respect to Happiness"

The sweets of Pillage can be known

to no one but the Thief,

Compassion for Integrity

Is his divinest Grief.

—Emily Dickinson (1830–1886), "Part Five: The Single Hound,"

Complete Poems

Identity Theft and Data Loss on Campus—Minimizing and Addressing Risk

James A. Keller, Esq., and Melissa Hill, Esq., Saul Ewing LLP

Abstract: The dawn of the cyber age has brought the development of new methods for obtaining, transmitting, and storing amounts of information more vast than the human mind can fully comprehend. Yet these advances in technology have also introduced their share of challenges, especially for colleges and universities who can now keep hundreds of thousands of constituent records in computerized systems. For these institutions, the threat of such information becoming compromised is very real. This article will discuss what is happening in regard to breaches of security, how it is happening, and what preventive measures institutions may employ to minimize the likelihood and impact of these cyber attacks.

Remember files? Those heavy metal things that stored paper, and that you could literally lock up behind a door? Once secured, it would take a Watergate-ian effort to get at those papers—and really, who would go through that trouble?

The information storage situation on your campus today is meaningfully different. You store everything electronically (perhaps with a hard copy backup), bolstered by pass code protection, encryption, or whatever the latest security audit suggests. And while this security has become quite good, it is, nonetheless, "virtual." Unlike a physical lock and key, virtual security can be compromised remotely by sophisticated ne'er-do-wells from almost anywhere on the planet, at any time. And in a final irony, while physical limitations of hard copy files necessarily limited your storage capabilities, the incredible memory capabilities of today's sophisticated systems allow you to store every detail about your thousands (or hundreds of thousands) of students, employees, faculty members, alumni, donors, and contacts. So, while you can store and quickly access amazing amounts of information, so can the bad guys.

While you can store and quickly access amazing amounts of information, so can the bad guys.

This reality has unfortunately hit home at some of our finest and seemingly best-prepared institutions: Ohio University (OU), The University of California at Los Angeles (UCLA), and The University of Colorado (CU), to name a few. While the specifics of each attack varied slightly, the basic pattern was the same: hackers improperly accessed protected information, including Social Security numbers and financial aid information, from university databases.

Now Happening at a University Near You

Ohio University had a tough 2006 on the IT front. On April 21, a cyber attack struck OU's Innovation Center's Technology Transfer Department. Thirty-five students had their Social Security numbers exposed in that data theft.[1] Just three days later, another breach occurred. The OU Alumni Relations database was the target of that data theft, and detailed information for more than 300,000 alumni and friends of the school was exposed.[2] Less than two weeks later, the university discovered a third incident of data theft in the school's health center, exposing more than 60,000 individuals' personal information.[3] In each instance, the hackers accessed and potentially "stole" names, Social Security numbers, and an array of other confidential information. Collectively, the 2006 events at OU comprised one of the largest cyber attacks ever inflicted upon a college or university.

The fall of 2006 brought the cyber attack scourge to UCLA. On November 21, 2006, technicians discovered a security breach in a database containing personal information of approximately 800,000 people. Worse yet, investigations revealed that the database had been illegally accessed on a routine basis since as early as October 2005.[4] UCLA officials announced the news on December 12, and

issued notification letters to potentially affected individuals, advising them of precautionary steps they should take to minimize the risks of identity theft and misuse of personal information.[5] Following an extended investigation, UCLA confirmed that these breaches resulted in the illegal retrieval of approximately 28,600 per-reference Social Security numbers. The university sent follow-up notices to those individuals on January 10, 2007, clarifying that the illegal retrieval of information did not necessarily mean the individuals were victims of identity theft, or that the Social Security numbers were being misused. Nonetheless, UCLA's acting chancellor reiterated, by separate letter, suggestions for preventing credit fraud and related crimes.[6] UCLA then went a step further and established a website providing facts, investigation updates, notification information, and fraud prevention tips.[7]

Around the same time in Boulder, Colorado, while students were finishing finals and packing to leave for winter break, university officials faced similar problems. On December 15, 2006, CU announced the discovery of a computer attack on one of its servers, exposing personal information of approximately 17,500 individuals.[8] The university notified those potentially affected, issued a press release, and provided identify theft prevention information to its community via an informational website.[9]

CU was attacked again in May of 2007. This time, a college of arts and sciences database was hit with a virus, exposing the names and Social Security numbers of almost 45,000 students.[10] CU technology security investigators discovered that the virus entered the university's server through a vulnerability in anti-virus software that was compounded because a security setting was not properly configured. In response, the university issued a press release,[11] sent precautionary letters to anyone whose information was stored on the server, and established a website informing students of how to protect themselves from identity theft.[12]

The drumbeat continued in April 2007, when administrators at the University of California, San Francisco (UCSF) began notifying both current and former students and employees about a possible computer data breach[13] after learning a server in the office of the president had been compromised. The server was immediately taken offline, notices were mailed to the affected individuals, and an identity theft website was established. Finally, as recently as June 2007, both the University of Virginia (UVA) and the University of Iowa (UI) were in the process of sending notifications to students and faculty members to advise them of security breaches. At UVA, a hacker broke into the school's network on 54 separate days, and the records, including names, Social Security numbers, and birth dates, of almost 6,000 faculty members were accessed. At UI, various electronically-stored records, including the Social Security numbers of approximately 1,100 per reference faculty members, students, and applicants to a graduate program were compromised. Both universities announced that they would take steps to notify affected parties and enhance network security.[14]

How They're Getting In (and Why)

Similar breaches occurred throughout 2006 and early 2007 at various colleges and universities across the country, from the University of Delaware[15] and the University of Texas,[16] to Vanguard University[17] and Johns Hopkins.[18]

How?

Simply put, the cybercriminals are finding a way in, and the information is getting out. From hacking into sophisticated technical servers, to compromising private information placed on public or non-secure websites, to the simple theft of a laptop and its files, schools are being attacked from a variety of different angles. Here are some of them.

The Unknown Server: In one of the most egregious OU attacks, hackers accessed a server in the alumni relations office that computing officials believed was offline. As the university learned following an investigation, the server had never been properly shut down and hackers discovered the active server still connected to the network. Although the hackers used the server primarily for sharing music files, it was connected to the broader OU network, and personal alumni and staff information was at risk of exposure the entire time.[19]

The Persistent Impostor: In the spring of 2007, a hacker retrieved personal information from more than 22,000 current and former University of Missouri at Columbia students through an online help desk. The hacker discovered an online form used by students to post information requests and track the status of those requests. Posing as a student, the hacker inundated the server with a number of online inquiries seeking to obtain campus-related

information, and ultimately was provided with a report that included the names and Social Security numbers of students who had worked in on-campus jobs.[20]

The Security Flaw: In the UCLA incident, the hacker discovered and exploited a flaw in database software that computer security technicians had not detected. The hacker continued to access the database for more than a year, seeking and retrieving Social Security numbers throughout the process.[21]

The Lost or Stolen Device: In 2006, a thumb drive containing student rosters was stolen from a professor at the University of Kentucky, and that simple theft exposed personal information from eight years of class rosters.[22]

Why Us?

While it is hard to say for sure, one can offer several reasons why campuses have become a favorite target of hackers.

Funding: Unlike for-profit corporations, for whom data loss can mean a hit to their bottom line, non-profit educational institutions have been historically less inclined to devote significant spending to secure their information or to upgrade and improve systems that collect and store a wealth of information.

Social Security Number as ID: Many schools have historically employed Social Security numbers as a student's identification number, or for a password that is used for everything from class registration to purchasing lunch. This increases the risk of fraud and identity theft.

Your Students May Be Putting You at Risk: College students have become sophisticated users of the latest computer technology and spend money on hardware and software faster, and in larger quantities, than the typical computer user.[23] This means more computer interaction with off-campus sources and, by extension, more points of vulnerability. If these students are making these contacts while connected to your server, the vulnerability of one can become a vulnerability of all.

Prevention and Mitigation

If you have been fortunate enough to avoid a cyber attack—or if the dust has just settled from an attack—your institution's primary focus should be on enhancing the protection of its computer network. This protection could include physical improvements to computer security, policy changes, and, possibly, "cyber insurance." These will be addressed in turn.

Physical Techniques to Improve Security[24]

Firewalls: A firewall is a barrier that keeps outsiders and their viruses from accessing your computer network. A firewall should be installed at every point where the computer system may come into contact with other networks, even via e-mail.

Bsystem Tests/Cyber Audits: Conducting vulnerability tests will help quantify your institution's level of data security risk. Experienced outside consultants can be retained for the specific purpose of acting as hackers—they will attempt to hack into your computer networks and, in the process of doing so, can determine where the systems are vulnerable and require upgrades. These tests, also known as "cyber audits," can also include website-based customer self-assessments, interviews with IT and security personnel, and remote network scans to test vulnerabilities in a system's firewalls, servers, and other network devices.[25]

Your institution's primary focus should be on enhancing the protection of its computer network.

Encryption/Scrambling Personal Information: Personal information such as Social Security numbers, birthdates, and addresses should be encrypted and/or separated from other sensitive information.[26] Allowing third parties to access students' records and view all personal information exposes the university to a significant risk of identity theft. Experienced IT personnel, including those already on your campus, should be able to help here.

Policy Changes to Improve Security

Draft or Revise Your Data Security Policy[27]**:** An institution-wide data security policy should be implemented, outlining methods by which individual employees and students can secure the computer network. This should include the creation of unique passwords (combination of letters and numbers, small caps and large caps), password changes on a routine basis, and an immediate process for

deleting user names and passwords of matriculated students and discharged employees.

Limit Use of Social Security Numbers: A very basic method to minimize illegal access to personal information is using identifiers other than Social Security numbers, particularly for students. Hackers are aware that student ID numbers are often nothing more than a Social Security numbers with an additional attached digit.

Preferred methods would be the use of partial Social Security numbers (e.g., the last four digits), a combination of other personal information (prior street addresses, parents' birthdates, etc.) jumbled together to create a unique identifier, or creation of a randomly-selected, institution provided ID number that does not correlate to anything else. To move in this direction, some institutions have drafted Social Security number policies intended to limit, and ultimately eliminate, the use of Social Security numbers on campus except where absolutely necessary. The University of Pennsylvania, for example, has adopted a draft policy (soon to be final) that "calls on staff, faculty, contractors, and agents of the above to inventory their online and offline Social Security numbers and reduce the above risks [associated with SSN# use] by, in priority order: (1) eliminating this data altogether, (2) converting it to PennID [a unique campus ID], (3) truncating the data to capture and display only the last four digits, [or] (4) when the complete SSN is clearly necessary, ensuring strict security controls to protect the full data."[28] This sliding scale plan—with complete elimination of Social Security numbers as the ultimate (but perhaps unattainable) goal, and strict controls on their usage as the minimum requirement—makes good sense.

Cyber Insurance? Of course, any discussion of risk mitigation must include insurance. A number of insurance companies have begun offering "cyber insurance" for organizations seeking protection in the event of data loss, data theft, or security breaches. To date, these policies may cover the following: (1) legal liability to the organization for security and privacy; (2) crisis management and notification costs associated with a security breach; (3) any losses resulting from funds paid to terminate the threat of a computer attack; (4) any expenses incurred as a result of a computer security breach; and (5) any cost incurred by an insured to restore information that is corrupted.[29]

These policies are, for most underwriters, in their infancy. Premium calculations can be difficult, and whether all underwriters will offer these policies, or whether they will offer them to what may be seen as "high-risk" educational institutions (and on what terms), remain open questions. Early indications are that the cost will be linked to the size of the student body. A 4,000-student institution, for example, may spend approximately $5,000 per year for $1 million in coverage.[30] A school with as many as 20,000 students may be able to obtain $3 million in coverage for $50,000 a year.[31] And in a slightly more complex policy structure, Lloyd's of London issued a cyber policy with a $70,000 premium to a non-disclosed 11,000-student private college. The policy limits were $1 million for claims brought by the school on its own behalf—typically for property damage to its computer system caused created by a virus or attack—and up to $3 million for claims brought by third parties against the school for identity theft/data loss, etc.[32]

A number of insurance companies have begun offering "cyber insurance" for organizations seeking protection.

If you are considering cyber insurance, you should have a security audit performed, as that likely will be a precondition for coverage. In addition to campus head count, your premium is likely to vary based on the outcome of the audit, and a low security score may result in denial of coverage or in an unpayable premium.[33]

There are other risk mitigation products to consider. Following a security breach involving a stolen USB drive, Louisiana State University (LSU) entered into a year-long agreement with a credit agency to provide its students, faculty, and staff with free credit report monitoring and up to $2,500 in identity theft coverage. LSU will pay the credit agency $150,000 for the one-year agreement.[34]

Your School Has Been Hit, So Now What?

You have performed a cyber-audit, adopted new data protection policies, analyzed your coverage options,

and tightened up your servers. Despite these efforts, your institution was just struck by a cyber attack. Now what?

Notification

In the event of a cyber attack on campus, an immediate investigation and response is critical. The faster students, alumni, and faculty know of potential exposures, the faster they can act to protect their identity and their credit. In addition to being good policy, in some states notification is legally mandated. Many states have enacted security breach notification laws that dictate when and how to notify potential victims of data security breaches.

By enacting the California Security Breach Information Act in 2003, California became the first state to mandate consumer notification for data security breaches where personal information has or may have been improperly accessed.[35] The California Act defines "personal information" to include Social Security numbers, medical information, driver's license numbers, bank account numbers, or credit card numbers. California requires notification to affected individuals of all security breaches involving unencrypted data.[36]

More than half of all states have subsequently enacted similar statutes based on the California model.[37] While not identical, these laws share common attributes:

What is covered: "Personal information" is almost uniformly defined as California first defined it, and a "data breach" is commonly defined as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business."

Timeliness of notice: In the event of a breach, institutions that own the compromised personal information must provide prompt notice to an affected state resident. In addition, if the breach occurs while the data is in the care of someone or an entity other than the data's owner, prompt notice must be given to the owner of the data.

Methods of notice: Typically, the state laws provide that notice may be satisfied by:

- Written notice through the mail
- Electronic notice in conformity with the Federal Electronic Signatures Act
- Substitute notice through e-mail, website publication, or major statewide news media if the costs of providing notice would exceed a certain threshold (such as $250,000), or if more than a certain number of individuals are affected, or if the institution does not have sufficient contact information
- The institution's own notification system, if it meets the timeliness requirements of the security breach notification law in question

Destruction of unneeded sensitive information: Institutions that no longer have a reasonable business or educational purpose for collecting and storing personal information must take reasonable measures to destroy or encrypt the information so that it is unreadable and undecipherable.[38]

In the event of a cyber attack on campus, an immediate investigation and response is critical.

P.R./Handling the Media

In addition to fixing your campus system, you may well need to fix your campus. A data breach will engender great consternation among your students, faculty, and alumni, and if it is a meaningful breach, the press may also get involved. You must be prepared to appease apprehensions and deal with the media.

There are several ways to attack this. For example, following a security breach in April 2006, the University of Texas opened a call center and assembled a response team to address inquiries and concerns.[39] Other schools have established websites to provide pertinent information and updates, as UCSF did in April 2007 in response to its attack.[40] And when the press calls, you want to be able to point to the panoply of protective measures you already had in place and those that you are putting in place, and be able to do so quickly. It is imperative to know what security you have, what it can (or cannot) do, and who is responsible for these issues on your campus.

The Fallout of An Attack

Financial Loss

Institutions faced with security breaches may suffer more than just the loss of data and reputational harm. First, the actual cost of responding to the attack takes a toll. Ohio

University estimates that it has spent more than $77,000 simply distributing letters to those individuals affected,[41] not to mention the cost of operating a response website and hotline, and investigating the breach. Because incidents of data theft often bring to light flaws, holes, and vulnerabilities in a university's data security systems, costs associated with upgrading technology and enhancing security are also inevitable.

Lawsuits

Civil lawsuits related to data theft are becoming more common, as state statutes designed to protect personal information and prevent identity theft are giving rise to civil claims. Employees have sued employers,[42] customers have sued financial institutions[43] and data storage companies,[44] and, at Ohio University, two graduate students sued the school for privacy violations stemming from data thefts from school computers.[45] Those students are seeking to have the litigation certified as a class action, and are demanding that the university pay for credit monitoring systems for the approximately 137,000 people whose personal information was compromised in the data theft.[46]

While claims are being filed, courts appear reluctant, at least for now, to recognize a cause of action for failure to protect personal information.

In one federal court action, bank customers sued the bank and four of its employees in connection with the alleged improper use of plaintiffs' personal financial information. The customers asserted violations of state and federal consumer protection statutes, violations of the federal Racketeer Influenced and Corrupt Organizations Act (RICO), as well as basic common law claims for conversion and negligence.[47] More specifically, the customers complained that the bank failed: "to implement and follow the security procedures; to protect the confidentiality of customer information; to guard against the misuse of that information; and to detect, report, and stop suspicious activities of employees."[48] The federal district court dismissed these claims, noting that the statutes at issue did not expressly provide for a private right of action to enforce privacy obligations, but instead left enforcement to state and federal regulators. Finding no legislative intent to create a private right of action, the court refused to imply one in the statutes or in common law and dismissed plaintiffs' claims.[49]

In another recent case, a federal district court in Arkansas dismissed class action allegations of failure to protect personal data brought against a data storage company. The court found the injuries alleged were merely speculative. While the breach had occurred, plaintiff had no evidence nor could she assert that her personal information was actually used in a way that harmed her. The case accordingly was dismissed because of plaintiffs' lack of standing.[50]

While the small body of case law to date is favorable, as the problem of identify theft and data loss continues to grow in the public consciousness, the legal landscape may change as well. It is not much of a stretch to see a negligence claim making it to trial: by requiring (employees/faculty/students) to use the university's servers, the university assumed a duty to make those servers safe. An alleged failure to secure those servers resulted in a cyber attack and was a breach of that duty. Because of that breach, harm resulted to the (employees/faculty/students). The case may not yet exist in your jurisdiction, but it is coming.

Conclusion

Cyber attacks are nearly impossible to prevent, but that reality will not appease concerned students, faculty, or alumni. Just as colleges and universities routinely take steps in the "real world" to protect their campus, an expectation is growing for identical protection in the "virtual world." And it can be done.

As discussed, protecting against identity theft and data loss is ultimately not unlike other risk mitigation on campus: identify the bad guys, identify what they are doing and how, and then take proactive steps to ward them off. While this is particularly difficult in the world of electronic data, where the technology is constantly changing, it is a necessary effort that will require your legal, IT, and risk managers to work together. Hopefully this article provides some assistance in that effort.

About the Authors

James A. Keller, Esq. is the Chair of the Higher Education Practice Group at Saul Ewing LLP, and a partner in its litigation department. He has handled a wide array of litigation matters arising out of complex

business disagreements, and has particular experience defending colleges and universities and advising higher education institutions on liability issues. Mr. Keller consistently handles the defense of major premises liability actions, ERISA claims, white-collar criminal matters, and reinsurance disputes. He has also served as an adjunct professor at the University of Delaware, where he taught undergraduate law courses.

Melissa Hill, Esq. is an associate in the litigation department and a member of the Higher Education Practice Group at Saul Ewing LLP.

Endnotes

1 Terms like data theft, data loss, and hackers have become part of everyday language in the field of data theft prevention. "Data loss" occurs when data is lost from a data-storage device in any manner, including misplacement, human error, hardware or software failure, or theft. See "What is Data Loss?," available at http://www.bostoncomputing.net/consultation/databackup/dataloss/.

"Data theft" is used to describe an incident in which information is illegally copied or taken from a business, institution, or individual. This type of information typically includes Social Security numbers, credit card information, and other personal information. See definition for data theft, available at http://www.computerhope.com/jargon/d/datathef.htm.

"Identity theft" refers to the crime in which an impostor obtains critical personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. See "What is identity theft?," available at http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci801871,00.html.

Acts of data theft and identity theft are often committed by "hackers," a slang term for a computer enthusiast with knowledge of computer programming. Hacker has taken on a more pejorative meaning and often refers to individuals who have gained unauthorized access to computer systems and databases. See definition of hacker, available at http://www.webopedia.com/TERM/H/hacker.html.

A database can refer to any collection of electronically stored information. See definition of database, available at http://www.webopedia.com/TERM/D/database.html.

When a hacker or other individual illegally accesses a database, the personal information stored on the database is said to be "compromised." In other words, when it is known or suspected that the personal information has been viewed or accessed by someone unauthorized to do so, that information has been compromised.

2 Alumni & Faculty/Staff Data Theft, May 1, 2006, available at http://www.ohio.edu/datatheft/alumni/index.cfm.

3 "Ohio University Continues to Take Steps to Secure Computer Systems Against Attempts to Breach University Databases," May 11, 2006, available at http://www.ohio.edu/outlook/05-06/May/485n-056.cfm; "Hudson Health Center Data Theft," May 11, 2006, available at http://www.ohio.edu/datatheft/student/index.cfm.

4 UCLA identity alert, available at http://www.identityalert.ucla.edu/index.htm.

5 UCLA notification letter, Dec. 12, 2006, available at http://www.identityalert.ucla.edu/ID_alert_letter.pdf.

6 UCLA follow-up letter, Jan. 10, 2007, available at http://www.identityalert.ucla.edu/ID_alert_followup_letter.pdf.

7 See http://www.identityalert.ucla.edu.

8 "CU-Boulder Reports Security Breach In College Of Arts And Sciences Advising Computer," Dec. 15, 2006, available at http://www.colorado.edu/news/releases/2006/437.html.

9 See "Facts About Identity Theft," available at http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf.

10 See "CU Boulder Arts and Sciences Server Hacked on May 12," May 22, 2007, available at http://www.colorado.edu/news/releases/2007/224.html.

11 Id.

12 See "CU Boulder Responds to Computer Security Incident," available at http://www.colorado.edu/its/security/aac052007/.

13 "Data Thieves Hit University of California, San Francisco," consumeraffairs.com, Apr. 5, 2007, available at http://www.consumeraffairs.com/news04/2007/04/uc_data.html.

14 "Two Universities Hit by Security Breaches," June 11, 2007, available at http://www.informationweek.com/software/showArticle.jhtml;jsessionid=JUBS1B3C4D454QSNDLQCKICCJUNN2JVN?articleID=199903218.

15 "Public Safety Reports Computer Security Breach," UDaily online, May 23, 2006, available at http://www.udel.edu/PR/UDaily/2006/may/breach052306.html.

16 "Unauthorized Access of Computer Records Discovered at The University of Texas at Austin," Apr. 23, 2006, available at http://www.mccombs.utexas.edu/datatheft/release_4.23.06.asp.

17 Vanguard University identity alert, Jan. 26, 2007, available at http://www.identityalert.vanguard.edu/notification.htm. http://www.ci.costa-mesa.ca.us/docs/pdpress/2007-01-26-Grant-Theft.pdf. The above reference has expired (NPW)

18 "Johns Hopkins Loses Data; Congress Aflutter," consumeraffairs.com, Feb. 7, 2007, available at http://www.consumeraffairs.com/news04/2007/02/jhu_data_breach.html.

19 See Paula Wasley, "More Holes Than a Pound of Cheese," *The Chronicle of Higher Education,* at A40, Sept. 29, 2006.

20 See "Hacking the Help Desk," May 9, 2007, *The Chronicle of Higher Education,* available at htttp://www.chronicle.com/wiredcampus/index.php?id=2056.

21 See Brock Read, "UCLA Warns 800,000 That a Hacker May Have Obtained Personal Information," *The Chronicle of Higher Education,* at A31, Jan. 5, 2007.

22 See Vincent Kiernan, "Two Incidents Put More Than 200,000 Students at Risk of Data Theft," *The Chronicle of Higher Education,* at A21, Jun. 30, 2006.

23 See James Martin and James E. Samels, "10 Trends to Watch in Campus Technology," *The Chronicle of Higher Education,* at B7, Jan. 5, 2007.

24 See Nick Brookins, "Seven Ways to Prevent Computer Hacking," Detroit Regional Chamber, available at http://www.detroitchamber.com/detroiter/articles.asp?cid=49&detcid=130; and Paul Freudenberg, "Take Precautions to Prevent Computer Hacking," *Portland Business Journal,* July 27, 1998, available at http://www.bizjournals.com/portland/stories/1998/07/27/focus8.html.

[25] NetDiligence is one such company that provides such "cybersecurity assurance services." See http://www.netdiligence.com/services.htm.

[26] Encryption is a process whereby individuals illegally viewing information on the computer network will not be able to view the personal information because it will be in an unreadable text, only viewable through the permitted key. Freudenberg, *supra* note 27.

[27] A data security policy establishes policies for management of a university's data and defines responsibilities for the protection of the data. Examples of adopted data security policies may be found at http://www.gsu.edu/security, Georgia State University's Security Awareness and Incident Prevention leaflet; and Institution Data Resource Management Policy, The University of Michigan Standard Practice Guide, at 601.12, available at http://spg.umich.edu/pdf/601.12.pdf.

[28] See http://www.upenn.edu/almanac/volumes/v53/n34/fc-ssn.html.

[29] Dan Briody, "Online Indemnity," Inc.com, April 2007, available at http://www.inc.com/magazine/20070401/technology-insurance-sidebar. This link has expired.

[30] Andrea L. Foster, "Worried About Hackers? Buy Some Insurance," *The Chronicle of Higher Education,* at A42, Oct. 13, 2006.

[31] Id.

[32] Id. Outside claims are typically claims concerning confidentiality with unsecured private information.

[33] Id. at A42.

[34] Andrea L. Foster, "LSU Arranges Identity-Theft Insurance for Students and Employees," *The Chronicle of Higher Education,* at A33, Sept. 22, 2006.

[35] Cal. Civil Code § 1798.82 (WEST 2007)

[36] Unencrypted data is at greater risk of being stolen and used for illegal purposes.

[37] An Act Requiring Consumer Credit Bureaus To Offer Security Freezes; C.G.S.A. § 36(a)-701(b) (Effective Jan. 1, 2006) [Connecticut]; Computer Security Breaches, 6 Del. C. § 12B-103 (Effective June 28, 2005) [Delaware]; Unlawful Use of Personal Identification Information, F.S.A. § 817.5681 (Effective July 1, 2005) [Florida] (providing for monetary penalties for failure to meet notification requirements); Personal Information Protection Act; IL ST CH 815 § 530/15; (Effective Jan. 1 2006) [Illinois] (act applies only to "data collectors," defined to include such persons as government agencies, public and private universities, and financial institutions, among others); Act to Protect Maine Citizens from Identity Theft, Notice of Risk to Personal Data, 10 M.R.S.A. § 1348 (Effective Jan. 31, 2006) [Maine]; Identity Theft Prevention Act, N.J.S.A. § 56:8-163 (Effective Jan. 1, 2006) [New Jersey] (act also imposes data disposal requirements and limits the use of residents' Social Security numbers); Information Security Breach and Notification Act, N.Y. Gen. Bus. § 899-aa (Effective Dec. 7, 2005) [New York] (violators of act subject to legal action by the state Attorney General); Identity Theft Prevention Act, N.C.G.S.A. § 75-60 (Effective Dec. 1, 2005) [North Carolina] (expanding definition of personal information to include bank account numbers, credit and debit card numbers, personal identification or PIN codes, and fingerprint and biometric data); Breach of System Containing Personal Information, Oh. St. § 1349.19 (Effective Feb. 17, 2006) [Ohio] (narrowing notification requirement to only in instances when it is reasonably believed that the breach caused or will cause a material risk of identity theft); and Breach of Personal Information Notification Act, 73 P.S. § 2301 (Effective June 20, 2006) [Pennsylvania] (narrows breach requiring notification to only incidents that are believed to have caused or will cause injury to a resident of the Commonwealth).

[38] Catherine M. Bump, et al., *Summary of State Data Security Laws as of March 2006,* 865 PLI/Pat 39, 43-44 (2006).

[39] http://www.mccombs.utexas.edu/datatheft/index.asp.

[40] "UCSF Establishes Identity Theft Website, Hotline," *USCF Today,* Apr. 4, 2007, available at http://pub.ucsf.edu/today/cache/news/200704043.html.

[41] Jim Phillips, "OU Has Been Getting an Earful About Huge Data Theft," *Athens News,* June 12, 2006, available at http://www.athensnews.com/issue/article.php3?story_id=25220.

[42] *Mannacio v. General Electric Co.,* Cal. Super. Ct., CV-065227 (Dec, 5, 2006). The plaintiffs, employees of the corporation, claimed that a stolen laptop resulted in theft of the unencrypted personal information of approximately 50,000 employees. The employees brought a class action suit asserting claims of negligence against their employer. The complaint alleged that the notice provided by the corporation of the breach was inadequate in that it did not provide sufficient information for those affected to protect themselves from improper use of the stolen information. The complaint sought full disclosure of the type of information accessed, as well a compensation for costs plaintiffs incurred in protecting themselves from identity theft. See "Data Breach Class Action Filed for Negligence Related to Stolen Laptop," Jackson Lewis, Dec. 14, 2006, available at www.jacksonlewis.com/legalupdates/article.cfm?aid=1039.

[43] *Smith v. First Century Bank,* No. 3:04 CV 591 (E.D. Tenn. 2005); see discussion *infra* at p. 15, n.53-54.

[44] *Bell v. Acxion Corp.,* No. 4:06CV0485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006). Defendant's information storage database was hacked and client files were compromised. The plaintiff, a client of the defendant, filed an action seeking damages, alleging defendant's lax security put her at risk of receiving junk mail and becoming a victim of identity theft. Id. at *1.

[45] "Who's suing OU right now, and why?" Jim Phillips, *Athens News,* Mar. 29, 2007.

[46] Id.

[47] *Smith v. First Century Bank, No.* 3:04 CV 591, 2007 WL 956652, *1 (E.D. Tenn. Mar. 29, 2007) (The district court dismissed plaintiffs' claims under the RICO statute for failure to allege sufficient evidence to establish necessary elements of RICO violations.).

[48] *Smith v. First Century Bank,* No. 3:04 CV 591, 2007 WL 1035125, at *2 (E.D. Tenn. Mar. 30, 2007) (alleging violations of the Gramm-Leach-Bliley Act (GLBA)).

[49] Id. at *3-4.

[50] *Bell,* 2006 WL 2850042, at *2. The district court did not address the specific question of whether a claim to recover damages resulting from a data security breach could survive had plaintiffs been able to demonstrate standing.

Last night a thief came to me

And struck at me with something dark.

I cried, but no one could hear me,

I lay dumb and stark.

When I awoke this morning

I could find no trace;

Perhaps 'twas a dream of warning,

For I've lost my peace.

—D.H. Lawrence (1885–1930), "Thief in the Night"

URMIA Presidents

1969–1970	**James R. Gallivan** University of Illinois
1970–1971	**Robert M. Beth** Stanford University
1971–1972	**Warren R. Madden** Iowa State University
1972–1973	**Stanley R. Tarr** Rutgers University
1973–1974	**Donald L. Thiel** University of Michigan
1974–1975	**Irvin Nicholas** University of California
1975–1976	**George A. Reese** Temple University
1976–1977	**James McElveen** Louisiana State University
1977–1978	**James A. White** University of Illinois
1978–1979	**David N. Hawk** Kent State University
1979–1980	**Dale O. Anderson** University of Iowa
1980–1981	**Charles D. Emerson** University of Kentucky
1981–1982	**Martin Siegel** New York University
1982–1983	**Truman G. Pope** Ball State University
1983–1984	**Alex J. Ratka** University of Southern California
1984–1985	**William O. Park** Northwestern University
1985–1986	**Eugene D. Marquart** California State Universities
1986–1987	**Thomas C. Halvorsen** University of Wisconsin
1987–1988	**John H. Walker** University of Alabama—Birmingham
1988–1989	**Mary Breighner** Columbia University
1989–1990	**Thomas R. Henneberry** Massachusetts Institute of Technology
1990–1991	**Leta C. Finch** Champlain College
1991–1992	**Benning F. Jenness** Washington State University
1992–1993	**Kathy M. Van Nest** Duke University
1993–1994	**Murray C. Edge** University of Tennessee
1994–1995	**Gregory P. Clayton** University of Nebraska
1995–1996	**Linda J. Rice** Clemson University
1996–1997	**George H. Meeker** Cornell University Medical College
1997–1998	**Gary H. Stokes** University of Delaware
1998–1999	**Glenn Klinksiek** University of Chicago
1999–2000	**Larry V. Stephens** Indiana University
2000–2001	**Leo Wade, Jr.** University of Southern California
2001–2002	**Larry V. Stephens** Indiana University
2002–2003	**Steven C. Holland** University of Arizona
2003–2004	**William Payton** University of Missouri
2004–2005	**William Payton** University of Missouri
2005–2006	**Mary Dewey** University of Vermont
2006–2007	**Allen J. Bova** Cornell University
2007–2008	**Ellen M. Shew Holland** University of Denver

URMIA Members Emeriti

Robert Beth, CPCU, CSP
905 Mears Court
Stanford, CA 94305-1041
E-mail: rpmb711@cs.com

Isaac Charlton
4027 Birch Lane
Fairbanks, AK 99709

Ernest L. Conti
102 Coventry Court
Moon Township, PA 15108
Phone: (412) 299-6881
Fax: (412) 299-6880

Mary Donato
University of New Mexico

Gerald Duncan
1639 1st Street SW
Minneapolis, MN 55112-3362

Murray C. Edge, ARM, CSSD
518 Shalamar Place
Irving, TX 75061-9408
Phone: (972) 313-9724
Email: murrayedge@email.msn.com

***Charles D. Emerson**
Lexington, KY

James R. Gallivan
1517 Waverly Drive
Champaign, IL 61821

Thomas C. Halvorsen, ALCM, ARM, AU, CPCU, BBA
24415 Amberleaf Court
Leesburg, FL 34748

George Harland
6248 Willow Avenue
Williamson, NY 14589-9706
Email: georgeharland@msn.com

Alice Horner, ARM
138 CO, Rt 14
Fulton, NY 13069

Thomas Henneberry
M.I.T.

***William Hustedt**
DeForest, WI

Benning F. Jenness
1077 Showalter Road
Moscow, ID 83843-9199

Mike Klein
Pennsylvania State University

Sandra LaGro
230 Larchwood Drive
Bowling Green, OH 43402
Phone: (419) 352-5400
Fax: (419) 372-0331
Email: dslagro@aol.com

Jack Leavitt
311 Corey Lane
Middletown, RI 02840-5661

Claudina Madsen
678 Arrowwood Court
Los Altos, CA 94022

Eugene D. Marquart
11270 Crocker Grove Lane
Gold River, CA 95670

William O. Park, MS, MBA, CPCU, ARM
111 Franklin Street
Geneva, IL 60134-2739
Email: wpark56683@aol.com

Janet Parnell, ARM
1142 Deercroft Ct.
Ft. Collins, CO 80525
Fax: (303) 871-4455
Email: jparnell4@juno.com

Patricia J. (Fowler) Payton, CPCU, ARM
Michigan State University

William A. Payton, DRM
University of Missouri

Truman G. Pope
5400 South Burlington Drive
Muncie, IN 47302-9606
Email: elipope@msn.com

***Alex J. Ratka**
Vancouver, BC CANADA

Harry E. Riddell
8333 Seminole Boulevard
Apt. 507B
Seminole, FL 33772-4394
Email: hhriddell@juno.com

James R. Roesch
510 East Beaumont Road
Columbus, OH 43214-2271

William F. Ryan
2548 Cross Country Drive
Port Orange, FL 32128

Martin Siegel
36 Country Club Drive
Jericho, NY 11753

Stanley Tarr, DHL
19 Hedge Row Road
Princeton, NJ 08540
Email: tnanat@aol.com

Donald Thiel
3660 Miller Road
Ann Arbor, MI 48103
Email: dlthiel@comcast.net

Kathy M. Van Nest, CPCU
Duke University

Leo Wade
University of Southern California

John H. Walker
273 Zodiac Drive
Alpine, AL 35014-6021

Jerre Ward
1812 Tupelo Trail
Holt, MI 48842
Email: jerreward3@juno.com

Robert B. Williams, CPCU, ARM
7 North Shaffer Drive
New Freedom, PA 17349
Phone: (717) 235-0502
Email: rwcw6@aol.com

Barbara M. Wolf
5216 Haskell Street
La Canada, CA 91011-1842

**Deceased*

Distinguished Risk Managers

No Date	**Eugene D. Marquardt** California State University System
	Lee Stenquist Utah State University
1989	**John Adams**
	Robert M. Beth Stanford University
	William O. Park Northwestern University
	John H. Walker University of Alabama, Birmingham
1990	**Thomas C. Halvorsen** University of Wisconsin, Madison
	Stanley R. Tarr University of Evansville
1992	**Mary Breighner** Columbia University
	Charles Emerson University of Kentucky
1993	**Murray C. Edge** University of Tennessee
	Leta Finch University of Vermont
1994	**Benning F. Jenness** Washington State University
	Claudina Madsen CPSJ Insurance Group
	William J. Wilson, Jr. Howard University
	Truman G. Pope Ball State University
1995	**James A. Breeding** Rutgers University
	Donald Thiel University of Michigan
1996	**Michael G. Klein** Pennsylvania State University
	Thomas R. Henneberry Massachusetts Institute of Technology
1997	**Kathy M. VanNest** Duke University
	Charles Cottingham University of Missouri
1998	**Leo Wade, Jr.** University of Southern California
1999	**George H. Meeker** Cornell University Medical College
2000	**Glenn Klinksiek** University of Chicago
	John E. Watson Pepperdine University
2001	**Rebecca L. Adair** Iowa State University
2002	**Larry Stephens** Indiana University
2003	**Paul Clancy** Boston University
	Mary Dewey University of Vermont
2004	**Christine Eick** Auburn University
	Elizabeth Carmichael Five Colleges
2005	**Jill Laster** Texas Christian University
2006	**Linda Rice** Clemson University
	Bill Payton University of Missouri
2007	**Allen J. Bova** Cornell University

The *URMIA Journal* is published annually by the University Risk Management and Insurance Association (URMIA), P. O. Box 1027, Bloomington, IN 47401-1027. URMIA is an incorporated nonprofit professional organization.

The 2007–08 *URMIA Journal* was edited by Jessica L. Allen, Wheaton College, 501 College Avenue, Wheaton, Illinois 60187; designed by Ellen Rising Morris of Eighth Day Creations, Wheaton, Illinois; and printed at Indiana University Printing Services, Bloomington, Indiana 47405.

There is no charge to members for this publication. It is a privilege of membership, or may be distributed free of charge to other interested parties. Membership and subscription inquiries should be directed to the National Office at the address above.

URMIA would like to recognize these contributors:

Jenny Whittington, *URMIA Executive Director*

Communications Committee:
Donna Smith, *Chair*
Rebecca Adair, *Past Chair*

URMIA Members:
Regina Beer
Allen J. Bova
Harsh S. Dutia
Anne N. Gregson
Lorna Jacobsen
Corrinne Kjelstrom
Vincent Morris
Jordana Ross
Fitzroy A. Smith
Nigel Wilson

When you reach the end of your rope, tie a knot in it and hang on.

—Thomas Jefferson (1743–1826)

Back cover: Washington, D.C.:
host city for the 2008 URMIA Conference,
September 10–14.
(Photo courtesy of Arlington Economic Development)

Washington, D.C.

Conference Host City September 10–14, 2008

URMIA

PROTECTING YOUR INVESTMENT
IN HIGHER EDUCATION

University Risk Management and Insurance Association

If undeliverable, return to:
URMIA National Office
P.O. Box 1027
Bloomington, Indiana 47402

Presorted Standard
U.S. Postage
PAID
Bloomington, IN
Permit No. 2