URMIA Journal

2015

Highlighting innovative and effective higher education risk management solutions.

UNIVERSITY
RISK MANAGEMENT
AND INSURANCE
ASSOCIATION

What we anticipate seldom occurs,

but what we least expect generally happens.

—Benjamin Disraeli (1804-1881),

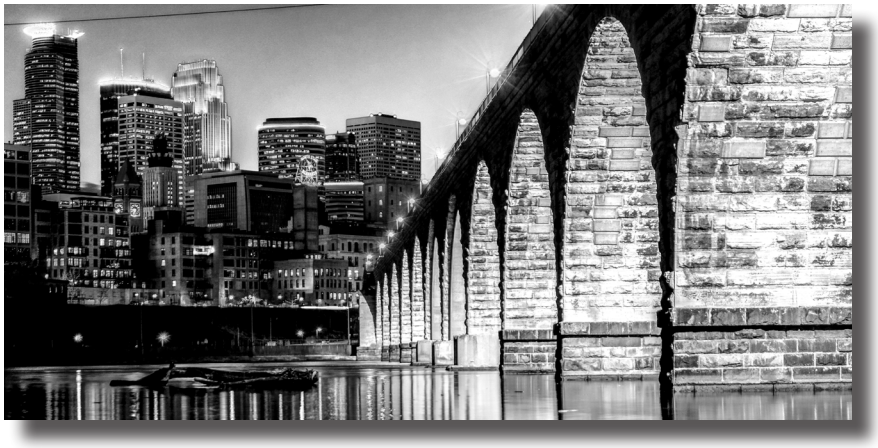
British Politician and Author

Table of Contents

URMIA Journal

2015

University Risk Management and Insurance Association



The host city of URMIA's 46th Annual Conference - Minneapolis, MN.

URMIA National Office
PO 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 Among Higher Education Risk Managers

OFFICERS

President
Marjorie F.B. Lemmon, ARM, CPCU
Yale University

President-Elect
Donna McMahon, MBA, MS
University of Maryland, College Park

Secretary
Kathy E. Hargis, MBA
Lipscomb University

Treasurer
Tish Gade-Jones
University of Nebraska System

Parliamentarian
Michael J. Gansor, CPCU, ARM, AAI, AU, AFSB, LUTCF
West Virginia University

Immediate Past President
Anita C. Ingram, ARM, MBA, MTS
Southern Methodist University

DIRECTORS

Sally Alexander, BA, LLB, MEPM, ARM ('16)
Colorado State University

Steve Bryant, CRM, ARM ('16)
Texas Tech University System

Luke Figora ('17)
Northwestern University

Leta C. Finch, MPA, DRM ('15)
Aon Risk Solutions

Samuel Florio, JD ('15)
Santa Clara University

Kewsic Joiner ('17)
Minnesota State Colleges and Universities

Kimberly Miller ('15)
Ball State University

Jordana Ross, ARM, CRM ('17)
Seattle Pacific University

Barbara Schatzer, MBA, ARM ('16)
University of San Diego

Lisa Zimmaro, Esq. ('16)
Temple University

From the President

Hello!

The *URMIA Journal* is the preeminent publication of URMIA, and, on behalf of URMIA's Board of Directors and Communications Committee, we present the 2015 issue. We are confident you will find it both enlightening and insightful.

The *Journal* represents the breadth and depth of the knowledge of our members, our staff, and our partners. It is the culmination of a great deal of effort by the committee and, in this particular issue, by 23 different contributing authors. The 13 articles contain a wide array of topics, including identifying risk, choosing the right risk management tools, liability for lightning at athletics events, building and tracking compliance programs in higher education, cyber security and responding to cyber incidents, student opioid use, liabilities in sports medicine departments, building an effective emergency response plan, and what enterprise risk managers and traditional risk managers can learn from each other. Plus, there is an article analyzing the eagerly awaited results of the URMIA Higher Education Risk Manager Salary Survey conducted in the spring of 2015, something that is especially relevant to all of us. And, we highlight the 2014 winner of the Innovative Risk Management Award! Congratulations to Allan Brooks and Chapman University!

URMIA's values emphasize that the organization is "pledged to the advancement of higher education risk management and the professional growth of our members." This publication is a true example of that, and I would like to thank the authors and the editors for their tireless work. So grab something to drink, a bowl of popcorn, and sit back, relax, and spend some time reading the *Journal*! You won't be disappointed.

We are looking forward to seeing you all at URMIA's 46th Annual Conference in Minneapolis this year! While you're there, please let us know what you think of the *Journal*!

Marjorie F. B. Lemmon, ARM, CPCU
Risk Manager
Yale University
URMIA President, 2014-2015

2015 *URMIA Journal* Sponsors

URMIA thanks each of the financial contributors who supported the publication of the 2015 edition of the URMIA Journal:

AIR Worldwide

World Headquarters
131 Dartmouth Street
Boston, MA 02116
617-267-6645
www.air-worldwide.com

AIR Worldwide is one of the world leaders in the development and application of mathematical models that assess the potential financial ramifications of natural and man-made catastrophes on property and life. In fact, AIR pioneered the very specialized field of probabilistic catastrophe modeling.

Our models—which today cover more than 90 countries and perils ranging from tropical cyclones, earthquakes, tornadoes, hail, flood, and terrorism—were first utilized by insurance and reinsurance companies, who are at risk of significant financial loss to their highly diverse portfolios. Applications of the technology have since broadened to serve a diverse audience, including governmental and quasi-governmental organizations.

Our credibility with such entities rests in no small part on the caliber of our staff, which is comprised of highly-qualified professionals representing the disciplines of meteorology and climate science, seismology and geophysics, wind and earthquake engineering, mathematics, statistics and actuarial science, insurance and reinsurance, and software engineering. A significant percentage of our technical professionals hold Ph.D. credentials in their field of expertise.

Kroll

600 Third Avenue, 4th Floor
New York, NY 10016
212-593-1000
www.kroll.com

In today's information economy, data can be your organization's most valuable asset, but with the rise of mobile technology, cloud computing and an exponentially growing volume of digital information, keeping that data secure also becomes one of your greatest challenges.

No one is immune to data loss incidents, and no one is better equipped than Kroll to help you identify and close gaps that put your organization's cyber security at risk. Information security issues — such as data breaches or employee misconduct — are a constant worry for C-suite leaders as well as for front-line managers in your organization. Cyber security challenges put sensitive data at risk and can cost your company time, revenue, and resources.

At Kroll we know securing and managing electronically-stored information (ESI) is critical to the future of your business. We offer end-to-end cyber security consulting, from information risk assessments that help you benchmark safety measures and shore up weaknesses, to penetration testing that checks for robust defenses. Our global team delivers scalable cyber security solutions to help you protect confidential and proprietary information from data security risks such as malicious insiders, network vulnerabilities, and inadequate security policies.

2015 *URMIA Journal* Sponsors

Riskonnect

1701 Barrett Lakes Blvd.
Suite 500
Kennesaw, GA 30144
770-790-4700
www.riskonnect.com

Riskonnect, Inc. is the provider of a premier, enterprise-class technology platform for the risk management industry. As an independent innovator in risk management technology, Riskonnect develops and markets a growing suite of technology solutions on a world-class cloud computing model, helping clients elevate their risk management programs, safety solutions, and programs for management of risks across the enterprise. Through Riskonnect RMIS, Riskonnect GRC, Riskonnect EHS, Riskonnect Healthcare, and other Riskonnect applications, the company provides the risk management industry with the specific, configurable solutions needed to reduce losses, control risk, and affect shareholder value.

Riskonnect, Inc. was founded in July 2007 by Chief Executive Officer, Bob Morrell; Vice President, R&D, Antonio Dabraio; and Vice President, Applications & Platform, Roger Dunkin. Independent and privately held, Riskonnect is Morrell's second entrepreneurial endeavor in the risk management software space. Using his expertise and best practices from the rapid growth and divestiture of his first successful organization, Morrell and his team have grown Riskonnect to be the work platform of choice among leading executives and risk and safety professionals.

TERRADOTTA

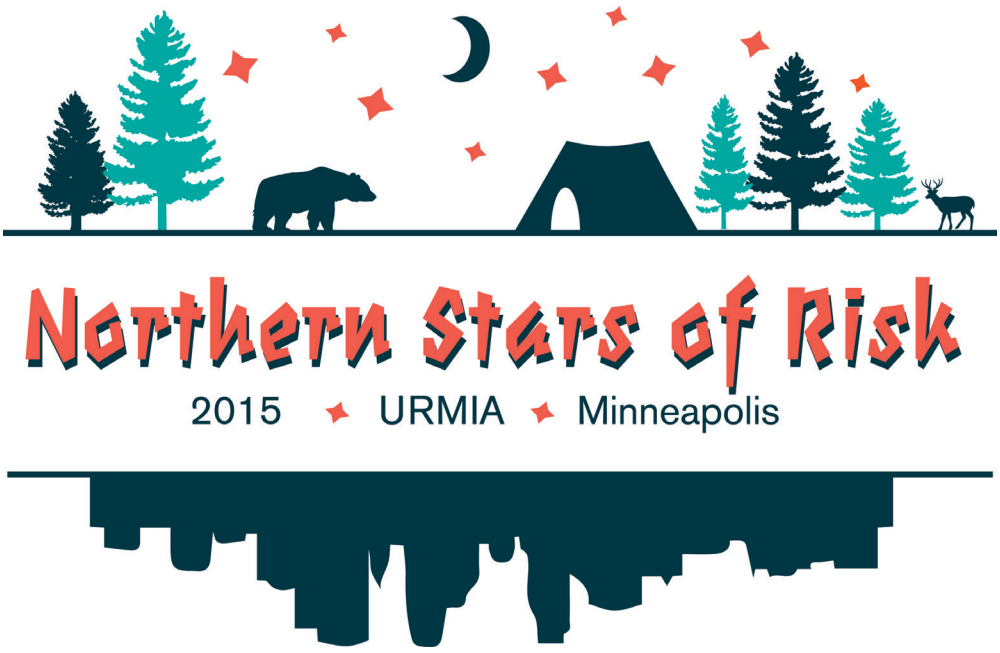
The Leading Software Platform for University Enrollment, Mobility and Risk Management

Terra Dotta

501 W Franklin Street
Suite 105
Chapel Hill, NC 27516
www.terradotta.com

Terra Dotta software mitigates risk by tracking student and faculty travel anywhere in the world. You can track study abroad travel, side trips, and incident reports; send emergency SMS text messages; and locate students, staff, and faculty instantly with Terra Dotta software. Our software manages the life cycle of enrollment management and allows your offices to be paperless and more efficient—while keeping your travelers safe. For more information, visit www.terradotta.com.

Upcoming URMIA Events



Join us **October 10-14, 2015**, in Minneapolis, Minnesota, for URMIA's 46th Annual Conference. Visit **my.urmia.org/annual2015** for more information, and use the hashtag **#URMIA2015** to connect with URMIA on social media!

URMIA's 4th Annual Risk Management Week is coming to your campus November 2-6, 2015! Gather your colleagues to spread the word about good risk management practices on campus, and help make everyone a risk manager!

Visit **my.urmia.org/rmweek** for tips on setting up your own RM Week events, resources to share with your campus, and daily webinars explaining risk management topics relevant to everyone at your institution.

Plans based on average assumptions are wrong on average.

—Samuel L. Savage,

Stanford University Professor and Author

Identifying Risk: A Survey of Practices in Higher Education

| *David Olson, The Master's College; Glenn Klinksiek, CPCU, ARM, MBA, DRM, URMIA*

Introduction

During the summer of 2014, a discussion was started about how risk managers discover new or emerging risks. As a result of this discussion, the University Risk Management and Insurance Association (URMIA) conducted a survey of its members in June 2014 to find out how this was done by practitioners in a real-world context. While some responses may seem intuitive and others beg for further investigation, the purpose of the survey was to open a dialogue; an opportunity for risk managers to challenge each other and to ask the question, "How well are you looking for the next emerging risk?"

Summary

URMIA's member survey received 126 anonymous responses. The results show that risk identification is a shared responsibility at almost every institution and that rarely do risk managers have sole responsibility for that step in the risk management process. While enterprise risk management models often mention the internal audit function as has having risk assessment responsibilities, only 15 percent of respondents say their process includes internal auditors. The lack of auditor involvement may be a missed opportunity.

Respondents generally believe their risk-identification processes will identify some emerging risks but not all. The high level of confidence in identifying emerging risk may suggest a general over-confidence as only a third of respondents specifically look for emerging risks. The lack of specific attention to emerging risk is surprising as the goal of risk identification is to find issues early on that may pose a threat to the institution's ability to achieve its goals.

The following is a summary of the survey results.

The purpose of this survey was to open a dialogue; an opportunity for risk managers to challenge each other and to ask the question, "How well are you looking for the next emerging risk?"

Survey Results

The goal of the survey, "Identifying Risk - A Survey of Practices in Higher Education," was to find out how risk managers anticipate new or emerging risks in their risk identification process. Risk identification is an essential part of any effective risk management program.[1] Risk managers especially need a process to find unknown or unappreciated risks, to evaluate these risks and then develop effective risk mitigations strategies. Institutions have long been aware of well-known risks, such as athletic injury, student alcohol consumption, fire, and many more, and have methods of addressing these risks. However, if the risk identification process had worked well, institutions may have been better prepared to address current hot-button issues such as concussions and campus sexual assault.[2]

Methodology

URMIA conducted a 10-question survey of college and university risk managers from May 26 through June 13, 2014, using SurveyMonkey. Members of URMIA's "Institutional Members" online discussion group, totaling about 1,500 individuals from more than 590 institutions, were invited to participate. A total of 126 anonymous responses were received.

Risk Identification Responsibility

An expected finding of the survey was that almost all respondents (98 percent) said that they had responsibility for risk identification. Risk identification is the first step of the commonly accepted risk management process of risk identification, assessment, mitigation, and monitoring.

What was unexpected is that nearly all respondents (95 percent) share the responsibility with others. Involv-

ing others in risk identification may improve the results through the involvement of professionals with exposure to different areas of the institution, with differing skill sets, and with differing perceptions.[3] More individuals looking out for risk issues will likely find more issues to be considered than a single individual or department could discover. Because no one person or unit has complete institutional knowledge and views risk from a single perspective, singular responsibility for risk identification is limiting in scope.

Nearly 40 percent of respondents indicated that a risk committee was involved in the risk identification process. Committee involvement at this level seems low considering that the trend of institutions to adopt an enterprise risk management process and that ERM processes usually involve a risk committee.[4] A committee also seems to be an appropriate structure to bring together those with responsibilities for risk identification in a formal way. Future surveys should ask how those who share responsibilities for risk identification collaborate other than the use of a committee.

The survey asked what units of the university were involved with risk management in the identification process. The top 10 departments mentioned in response to this question comprise about 80 percent of the responses. The top 10 are shown in "Table 1 – Departments Sharing the Responsibility for Risk Identification." "All departments" was mentioned 19 times, apparently because those institutions feel that all department heads are responsible for identifying the risks in their area. This opinion is shared by COSO which states, "Everyone in an entity has some responsibility for enterprise risk management."[5]

The fourth most frequently mentioned unit with risk identification responsibilities is internal audit. However, internal audit was mentioned by just 15 percent of respondents. This is intriguing as models for enterprise risk management often place internal audit in a key role. According to the Institute of Internal Auditors (IIA) and the Risk and Insurance Management Society (RIMS), "The IIA and RIMS believe that collaboration between the disciplines of internal audit and risk management can lead to stronger risk practices in meeting stakeholder expectations. The two functions make a powerful team when they collaborate and leverage one another's resources, skill sets, and experiences to build risk capabilities within their organizations. The adage, 'the sum is greater than the parts,' certainly applies. And it is clear that leading organizations have discovered efficiencies, better decision making, and improved results by forming strong alliances between the risk management and internal audit functions."[6] The lack of participation with internal audit could indicate that smaller institutions do not have the resources to maintain an internal audit function. Whatever the reason, this low response concerning internal audit is troubling and could indicate either a lack of participation in the assessment process on the front end or a potential lack of risk management implementation monitoring on the back end. If institutions are not using both risk management and internal audit in the risk identification process, they are clearly missing an opportunity to conduct a more efficient and comprehensive approach to this critical activity.

Risk identification is the first step of the commonly accepted risk management process of risk identification, assessment, mitigation, and monitoring.

Risk Identification Process

Risk managers do not rely on one approach to risk identification. All respondents said they use two or more methods. "Table 2 – Risk Identification Techniques" shows the popularity of the eight methods listed in the survey and "Table 3 – Other Risk Identification Techniques" shows other approaches risk managers use.

Nearly three-quarters of the respondents use inquiries from campus units as an opportunity to identify risk. The fact that the most frequent method of assessment is people reaching out to risk management behooves risk managers to be accessible to campus units and to be seen as a credible resource. If risk managers are not consulted and the units forge ahead without building risk management into their activities, critical risks may not be identified or adequately managed. Interestingly, fewer than half the respondents take the initiative to look for potential risks by scanning internal resources.

Questionnaires are used by only a quarter of respondents to identify risk, much less than other approaches which use active engagement. While questionnaires could potentially result in a more thorough investigation of risk, the potential for poor or even negative response may prevent more risk managers from using them. Future surveys should explore risk managers' motivations when choosing identification methods to determine what effects this may have on risk identification. Certainly, questionnaires can be time consuming to create and require a daunting amount of effort to collect responses.

More than two-thirds of the respondents (68 percent) do not take steps designed specifically to look for emerging risks. Identifying areas of potential risk, no matter how theoretical, should be an important part of the risk identification process. This is especially necessary to respond to governing boards when they ask "what downside risks are we leaving out, and what opportunities are we missing? Imagine the unimaginable…"[7] If found, institutions can begin to address them early on. Still, the risk identification process must be strategic in its scope and structured to take into account what might be waiting over the next hill. As Janice Abraham said in *Risk Management: An Accountability Guide for University and College Boards* "enterprise risk management is a business process, led by senior leadership, that extends the concepts of risk management and includes… consistently scanning for emerging risks."[8]

Respondents are generally positive about their risk identification process. On the optimistic end, 12 percent are "confident important emerging risks will be identified." Sixty-eight percent "expect some emerging risks will be overlooked." On the negative end, 20 percent feel their risk identification process "probably will overlook important emerging risks."

Does the generally high level of confidence that the risk identification process will identify emerging risks suggest that respondents are over-confident in their processes? Only a third of total respondents specifically look for emerging risks including several respondents in the most optimistic group. Clearly emerging risks can be found without specifically looking for them. However, those charged with responsibilities for risk identification should be specifically thinking about what else could adversely impact the institution. Not doing so is a missed opportunity to improve the risk identification process.

Risk Identification Methods

To identify emerging risks, respondents use multiple methods that, in general, depend on others to recognize emerging areas of risk. Only one respondent in five use their imagination to think of new threats. "Table 4 – Approaches to Identify Emerging Risk" shows the responses to the choices offered in the survey and "Table 5 – Other Approaches to Identifying Emerging Risk" shows collaborative methods respondents use to identify emerging risk.

Nearly all of the respondents are confident that URMIA will provide adequate information regarding emerging risks. This is not surprising considering the survey was directed at URMIA members. NACUBO was another significant source of information, but only 10 percent of respondents look to the internal auditors association, Association of College and University Auditors, for help. This infrequent use is consistent with lack of participation internal audit plays in respondents' risk identification processes. "Table 6 – Publications of Associations Read for Risk Issues" lists the responses for the choices offered in the survey while "Table 7 - Other Association Publications Read" lists the sources respondents provided.

Most respondents look beyond higher education sources for emerging risks. About 60 percent say they discuss risk with risk management professionals from outside higher education. More should consider doing so as emerging risks may first be identified by risk professionals outside of higher education. The possibility outsiders may see risks in education before insiders motivated the University of Alberta to hold "an annual expert forum to review institutional strategy and risks. The experts, mostly from outside the university, bring a fresh set of eyes and unbiased perspective to key areas of university risk, in particular identifying important external developments that could affect the university."[9]

Emerging Risk Identified

The survey asked respondents to list emerging risks that their risk identification processes found. Over 70 percent of the respondents listed one or more risks they identified. "Table 8 – Areas of Emerging Risks" lists the 55 areas of risks that were provided.

The fact that respondents were able to list areas of new concerns that their processes identified shows that risk managers have new areas of risk on their mind and that

Department	# of mentions
Safety/EH&S	29
General Counsel/Legal	24
All Departments	19
Internal Audit	16
Public Safety/Security/Police	14
Facilities	12
Finance/Business/CFO	8
Student Affairs	8
Human Resources	7
IT/IT Security	6

Table 1: Departments sharing the responsibility for risk identification.

Answer Options	Response Percent
Requests for guidance from university faculty and staff (usually framed "My boss told me I should call you" leading to the question "what do you think of…")	73.6%
Interviews with key persons (one or a couple at a time)	70.4%
Surveys and inspections	70.4%
Insurance application responses	66.4%
External reviews (brokers, audit firms, others)	58.4%
Facilitated group discussions	48.8%
Scans of internal resources (website, phone book, newsletters, etc)	40.0%
Written questionnaires	25.6%

Table 2: Risk identification techniques.

Technique	# of mentions
Scanning external resources	7
Claims and claims trends (internal & external)	4
Informal campus conversations	2
Emergency management plans	1
Reactive	1
Anonymous reporting system	1
Local papers	1
Risk management review/contract review	1
Campus "expert forum" with external resources	1
Standing committee	1
Broker risk assessment survey	1
Internal audits	1
Luck	1

Table 3: Other risk identification techniques.

Answer Options	Response Percent
Blue sky imagination	20.8%
Read newspapers, higher education publications (Chronicle of Higher Education, etc) with an eye to potential issues	79.2%
Read publications of higher education associations with for new issues	81.6%
Read publications by insurance companies, brokers, audit firms for new concerns	72.8%
Discuss risk with risk managers at other organizations looking for issues you haven't previously considered	76.0%

Table 4: Approaches to identifying emerging risks.

Emerging Risk Identification	# of Mentions
ERM process	8
Outside sources (insurance, trade)	6
Dialogue with depts.	6
Tactical plan review	6
Strategic plan review	5
Survey/focus groups	2
Emergency management plans	1
Outside consultant	1

Table 5: Other approaches to identifying emerging risks.

Answer Options	Response Percent
URMIA	98.4%
NACUBO	65.1%
NACUA	34.9%
ACUA	10.3%

Table 6: Publications of associations read for risk issues.

Answer Options	# of mentions
Association of Governing Boards of Universities and Colleges (AGB)	2
United Educators Insurance (UE)	2
National Association of Independent Colleges and Universities (NAICUA)	1
American Council on Education (ACE)	1
Education Advisory Board	1
NAFSA: Association of International Educators	1
Western Association of College and University Business Officers (WACUBA)	1

Table 7: Other association publications read for risk issues.

Risk Area	# of mentions
Cyber risk	23
International risks	16
Minors	11
Compliance	8
Title IX and sexual assault	7
Students	7
Concussions	6
Emergency planning/management	5
Athletics	5
Enrollment (diversity, declining, access, pre-college)	3
Nanotechnology	2
Unionization (part-time faculty, students)	2
Student substance abuse	2
Fiduciary liability	2
Climate change	2
Drones	2
Energy (reduction in use, supply volatility)	2
Exports	2
Student practicum	2
Succession planning	2
Tuition (caps, declining)	2
Healthcare reform	2
Incidental/miscellaneous professional liability	2
Gaps in antiquated processes	1
Watercraft rental	1
Contract risks	1
Fraud	1
Faculty conflict of interest	1
Cost cutting measures	1
Community expansion	1
Rate of technological change.	1
Data integrity for decision making	1
Governmental funding changes.	1
Medical malpractice from changing practices	1
Risk from new income sources	1
Lack of risk culture	1
On-line education	1
New accreditation organizations	1
Declining research funding	1
Facility use by outsiders	1
Pandemic	1
Off campus programs	1
Inability of organization to adapt to new realities	1
Disruptive Forces in Higher Education	1
Effects of changing marijuana laws	1
Vehicle fleet	1
Hallway hazards	1
Active shooter/terrorism	1
Building access	1
Worker health	1
Substance abuse	1
Fall hazard	1
E-cigarettes	1
Volunteers	1
Video use	1

Table 8: Areas of emerging risk.

risk managers are constantly thinking about whether these new areas comprise the entire changing risk landscape within their context. Many of the "emerging risks" provided by respondents are already known and appreciated in the risk management community. Some respondents have identified risks that are not often listed by institutions as areas of concern in the authors' experience and therefore could be considered emerging risks for higher education. These risks are shown in italics in Table 8.

Conclusion

Are risk managers aware that risks can change over time? Yes. The fact that 70 percent have at least one new risk on the horizon shows that the reality of change is well recognized by the risk management profession. This survey even highlights the great foundation that is being laid by the 32 percent who already look for emerging risk within their assessment process. The message of this survey:

(1) If you are not looking for emerging risks in your assessment process you should consider doing so. The breadth of knowledge and experience brought by the other departments involved would enhance the ability to look for what is around the corner.

(2) If there is an internal audit function at your institution that is not involved in the assessment process, consider including it in the next meeting. This will bring value to your assessment and give internal audit a better grasp on what to monitor.

(3) Let us not be too confident. There will always be the black swan events, but we should never use that as an excuse for not finding what can be discovered.

Let us not be too confident. There will always be the black swan events, but we should never use that as an excuse for not finding what can be discovered.

About the Authors

David Olson is a 2017 MBA candidate at the University Of Wisconsin School Of Business. While at UW, Mr. Olson will be specializing in risk management and insurance. Until recently he was employed at The Master's College in Santa Clarita, California. As the assistant director of campus safety, Mr. Olson oversaw department administration, emergency planning, workplace safety, and risk advising across campus. He enjoys helping strategic decision makers understand and plan for uncertainty.

Glenn Klinksiek headed the University of Chicago's risk management function for 25 years, retiring in 2012 as its associate vice president for risk management and audit. His responsibilities included directing the university's risk management and safety programs for the education, research, and healthcare enterprises. He managed its insurance and self-insurance programs; oversaw the university safety programs including laboratory, occupational, fire and life, vehicle, and radiation and environmental; maintained the emergency preparedness plan; managed its risk-based internal audit program; managed the compliance hotline and investigations; and staffed the university's compliance committee. Mr. Klinksiek holds a BS from the University of Wisconsin and an MBA from Indiana University.

Endnotes

1 "A robust risk assessment process forms the foundation for an effective enterprise risk management program." "A Practical Guide to Risk Assessment: How Principles-based Risk Assessment Enables Organizations to Take the Right Risks," PricewaterhouseCoopers, December 2008, page 5. In addition both COSO and ISO include risk identification as the step within their enterprise risk management models (cf. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management – Integrated Framework*: Executive Summary. 2004, page 4-5 and ISO 31000:2009, *Risk Management—Principles and Guidelines*. Geneva: International Standards Organisation, 2009).

2 Risk assessment includes filtering information for possible consequences that could present risks. Information that if well considered could have indicated that concussions and campus sexual assault were risks. According to a *USA Today* article published 7/29/14, "NCAA settles head-injury lawsuit" (http://espn.go.com/college-sports/story/_/id/11279710/ncaa-settles-head-injury-lawsuit-create-70-million-fund) states that in 2004, over a decade ago, the international community came to consensus on concussion management through a conference in Zurich. However, the

NCAA did not implement those standards." In 2004, people realized that concussed athletes should never return to play that day and that certain steps needed to be taken before they could return to play."
According to an NPR Education article, "The History of Campus Sexual Assault" by Anya Kamentez published on November 30, 2014 (http://www.npr.org/blogs/ed/2014/11/30/366348383/the-history-of-campus-sexual-assault), in 1957, a study "Male Sex Aggression on a University Campus" by sociologist Eugene Kanin posited a model where men used secrecy and stigma to pressure and exploit women. Mary Koss, professor of psychology at the University of Arizona, coined the term "date rape" back in the 1980s. A 1987 national survey of college men on the topic found that 7.7 percent of male students volunteered anonymously that they had engaged in or attempted forced sex and that almost none considered it to be a crime.

[3] "ERM creates an environment of collaboration. It encourages dialogue at all levels and between all disciplines on campus. Everyone who is involved in the process gains from the experience. The identification of risk takes on new meaning and understanding. The decisions that are made with respect to the management of risk are more robust and comprehensive." *Enterprise Risk Management: A Fundamental Practice for Higher Education*; Jane Dickerson, Peter J. Fallon, Leta Finch, *URMIA Journal 2003-2004*, page 27.

[4] See Step 9 of the "Road Map for a Phased Approach to Drive the ERM Process," *Road to Implementation: Enterprise Risk Management for Colleges and Universities*, Gallagher Higher Education Practice, page 22.

[5] *Enterprise Risk Management-Integrated Framework* Executive Summary, September 2004, Committee of Sponsoring Organizations of the Treadway Commission, page 6.

[6] *Risk Management and Internal Audit: Forging a Collaborative Alliance*, Risk and Insurance Management Society and Institute of Internal Auditors, 2012, page 3.

[7] See Action Step 7, "The State of Enterprise Risk Management at Colleges and Universities Today," Association of Governing Boards of Universities and Colleges and United Educators, 2009, page 3.

[8] Abraham, Janice M., *Risk Management: An Accountability Guide for University and College Boards*, AGB Press, 2013, p. 6.

[9] *A Practical Approach to Institutional Risk Management: Getting Risk Right in an Era of Constrained Administrative Resources*, The Advisory Board Company, 2012, page 61.

Like a well-prepared meal at a fine restaurant, ERM is best taken one course at a time, not mixed up on a single, giant plate.

—Joanna Makomaski and Beaumont Vance,

Authors of *Enterprise Risk Management for Dummies*

The Two-Headed Monster of Risk:

What Higher Ed Traditional Risk Managers and Enterprise Risk Managers Can Learn from Each Other

Andrew Goldblatt and Hans Gude, University of California, Berkeley

Introduction

The risk manager at the University of California, Berkeley, is always busy. How could it be otherwise on a campus with a brilliant but sometimes mercurial faculty, 36,000 activist students, a global research footprint, a dispersed fleet of over 500 vehicles, and a deferred maintenance backlog in the hundreds of millions of dollars?

So when the campus committed itself to an enterprise risk management program, the risk manager's first question was, "How far along with cloning is the genetics department? Because you're going to need two of me to get this done."

His second question was, "Oh, and by the way, what exactly is enterprise risk management?"

That was senior leadership's cue to bring in a director of enterprise risk management.

Although the addition of an enterprise risk manager was a necessary step, confusion over turf could have led the traditional risk manager and enterprise risk manager to rage across the campus like Godzilla and Mothra, destroying everything in their path in a struggle for dominance. Instead, they learned that traditional and enterprise risk management are distinct yet overlapping endeavors that can make each other more effective.

Although the addition of an enterprise risk manager was a necessary step, confusion over turf could have led the traditional risk manager and enterprise risk manager to rage across campus like Godzilla and Mothra.

Background

By traditional risk management we mean a more operational approach to risk, focused mainly on insurable risks.

By enterprise risk management we mean a more strategic approach to risk that focuses on risks that could jeopardize the campus's ability to achieve its objectives.

Typically, the traditional risk manager's job is to reduce the likelihood of insurable losses and then to handle claims and lawsuits when loss prevention efforts fail. The principal objective of the traditional risk manager is to get the campus through the day unscathed – or, in the alternative, minimally scathed. Although the traditional risk manager's loss prevention efforts are a form of enterprise risk management, their scope is usually limited to the operational arena: contract review, event planning, employee training, etc.

Typically, the enterprise risk manager's job is to help the organization's leadership manage (accept, avoid, share, or mitigate) risks that could erode the campus's ability to achieve strategic objectives and also to help leadership incorporate a risk perspective into decisions regarding new opportunities. The principal objective of the enterprise risk manager is to help the campus stay on the course it laid out in its strategic plan, which for Berkeley means maintaining its outstanding academic ranking.

On some campuses, the traditional risk manager and enterprise risk manager are the same person. Those who combine the positions are the unsung heroes of higher education risk management as they either have or must learn two distinct backgrounds and skill sets (*see table on page 18*).

At smaller schools, it makes budgetary sense to combine the two positions, even if the employee doesn't have both backgrounds and skill sets. But at larger, more complex schools, gaps in background and skills become more glaring, exposing the employee's weaknesses and perhaps increasing the school's risk as a result. Thus the tendency at most schools to assign the traditional and enterprise risk functions to different people and sometimes to different offices.[1]

At the University of California, Berkeley, the traditional risk manager and enterprise risk manager both belong to the Office of Ethics, Risk, and Compliance

Services, which reports to the Chancellor's Office and also includes the Title IX, whistleblower, privacy, public records, and ADA compliance functions.

Berkeley's traditional risk manager and enterprise risk manager started their positions in late 2011 after holding different risk-related jobs on campus. Initially they each did their own thing. Then they were put in the same office. They soon discovered they both had a liberal arts background, which led to freewheeling chats about art and philosophy. Eventually those chats turned into serious discussions about how best to manage risk in higher education. It helped that neither was content with the conventional approach to his field and was open to fresh ideas.

Benefits of Collaboration for the Traditional Risk Manager

The most important lesson the traditional risk manager learned from the enterprise risk manager is that it's crucial not to get lost in the weeds – that a traditional risk manager needs to evaluate risks not in terms of the attention they demand but in terms of their potential impact on the organization. Yes, it matters that professor X's subaward agreement has the best possible insurance and indemnification language and that professor X is insisting the subaward agreement be signed today, but is that as important as making sure the power supply to professor X's lab is uninterrupted or preparing professor X's lab for an inevitable natural disaster? In a job where time and resources are limited, having an enterprise risk manager's sense of priorities can focus the traditional risk manager on the most crucial risks, i.e. those most likely to threaten the campus's overall mission.

Along those same lines, the enterprise risk manager reinforced to the traditional risk manager that the name of the game is loss prevention, and that to the degree possible, the weight of claims management should be shifted to office colleagues and a third party administrator so the traditional risk manager has more opportunity to stop bad things before they happen.

In terms of fresh ideas, the traditional risk manager had long preached that everyone on campus is a risk manager but had limited his audience to staff and faculty. Students were seen as other. That's the conventional wisdom among traditional risk managers, who keep a wary eye on students as potentially adverse parties in claims and lawsuits. But education is a university's core mission. Seeing students as other can inhibit the mission.

	"Traditional" Risk Management	"Enterprise" Risk Management
Risk Focus:	Insurable risks	Strategic risks
Objective:	Protect the university from incidents that may result in large financial loss	Protect the university from events that may threaten its ability to achieve its strategic objectives
Helpful Background / skills:	• Insurance • Legal • Crisis management • Broad knowledge of business operations • Comfort in gray areas • Ability to negotiate • Ability to foster change • Ability to communicate to broad audience	• Accounting / finance • Professional services consulting, including organizational change and process improvement • Sales • Networking • Comfort in gray areas • Patience to accept slow, incremental change • Ability to communicate to leadership
Helpful Knowledge:	• Insurance policy details • Historical losses to the campus • Loss prevention techniques	• ERM frameworks • Risk theory • Quantitative business methods

Figure 1: Ideal background and skill sets for traditional and enterprise risk managers.

By enlisting students as risk managers, the traditional risk manager can surmount longstanding barriers to reducing student-related operational risks and contribute to the campus's co-curricular educational efforts by giving students their first lessons in risk awareness, loss prevention, and insurance.

The traditional risk manager now heads Berkeley's Compliance and Enterprise Risk Subcommittee on Student Risk. He is working alongside students in the effort to reduce alcohol-related medical transports, injuries, and deaths – a role he would not have imagined for himself three years ago. And when he asks senior management for resources to support the committee's efforts, he doesn't just make the traditional risk argument that students' families are increasingly disregarding well-established law regarding in loco parentis and holding the campus legally responsible for students' poor personal choices. He also makes an enterprise risk argument: that to continue attracting the highest-caliber students, the campus needs to address public perceptions that it condones a wanton, potentially lethal social environment.

Benefits of Collaboration for the Enterprise Risk Manager

By sharing an office with the campus's traditional risk manager, the enterprise risk manager has been exposed to the continual stream of telephone calls between the traditional risk manager and campus stakeholders seeking immediate, specific, actionable guidance about a multitude of risks—risks that either just happened, were about to happen, or would likely happen soon if not dealt with immediately.

Exposure to those conversations has helped the enterprise risk manager appreciate that traditional risk management has an exigency that a stand-alone, isolated enterprise risk manager might not otherwise perceive and at best understand only conceptually. This is the difference between a captain on the battlefield and a colonel at headquarters only remotely connected to the front lines.

As an example, although the enterprise risk manager may not participate in a meeting with, say, the chair of the Physics Department concerning power outages affecting the department's ability to conduct research (as the traditional risk manager would), learning about that specific, tangible, emerging risk from the traditional risk manager helped the enterprise risk manager understand the importance of reliable power sources to the campus's ability to achieve its research mission.

UC Berkeley is a large, complex living organism composed of thousands of moving parts. All the risks inherent in the organization, whether financial, operational, or reputational, live in the movement of those parts. Proximity to the traditional risk manager taught the enterprise risk manager that to be successful, enterprise risk management (ERM) has to make a difference on the ground—it has to understand and incorporate all those moving parts.

Another way to say this is that ERM must be pragmatic. The word is used deliberately here for two reasons. First, because it means to solve problems sensibly and realistically using an approach based on practical rather than theoretical considerations. Second, because it resonates with the campus's enterprise risk manager, a philosophy major who embraces the slogan of the 19th century "pragmatic" philosophers: "If it doesn't make a difference here (in our daily lives), then it doesn't make a difference there (in your intangible, unseen metaphysical world where angels are said to dance on the heads of pins)." If the enterprise risk manager can't help the campus make better decisions about where to apply scarce risk mitigation resources, then it doesn't make a difference what the campus's risk philosophy and risk appetite statements say.

Practical versus theoretical is easier said than done, because that is exactly the greatest challenge to implementing ERM. How does an enterprise risk manager find a way to descend from the general, theoretical principles articulated in the COSO guidance and become grounded in the day-to-day operations of a campus?

The perspective gained by exposure to a day in the life (actually, many days in the life) of the traditional risk manager has helped steer the enterprise risk manager toward a novel approach to implementing ERM at Berkeley that bridges the chasm between theory and reality, achieving a solution that can make a difference on the ground.

The enterprise risk manager has elected to base the ERM process in the activities (those "moving parts") Berkeley carries out every day across the campus in support of its mission of teaching, research, and public service. Working within the campus ERM governance structure, he identified the principal activities the campus

carries out, determined how essential those activities are to achieving the mission, identified the risks inherent in the activities, and assessed how well the risks are being mitigated. Having completed this process, the enterprise risk manager was in a position to make specific, tangible recommendations to leadership about where to focus resources. Delivering energy to the campus emerged as a top strategic risk.

Another way collaborating with the traditional risk manager helped the enterprise risk manager become clearer about how to implement ERM at Berkeley was in determining risk mitigation priorities. The enterprise risk manager came to Berkeley from the private sector, which invented ERM principally for financial risks. In the private sector, most decisions and priorities can be ranked and compared using the overriding metric of dollars. Even though he recognized that dollars are not the principal metric in the public sector, the enterprise risk manager initially had difficulty understanding why some campus risks, such as student alcohol abuse, appeared to be receiving attention and resources out of proportion to their potential to adversely affect the organization's ability to achieve its strategic objectives, especially when weighed against the risk of an unreliable power supply for the Physics Department, which endangers the research mission. The logic of his profession impelled him to recommend spending those funds to improve campus utilities first, and to assign a lower priority (possibly much lower) to funding efforts to reduce student binge drinking.

Until, that is, the enterprise risk manager recognized that attracting the highest-caliber students and doing everything reasonably possible to assure good outcomes for them are part of the campus's bottom line – and that parents' confidence in the campus rests in good part on the ability to assure the public that the campus cares about its students and effectively addresses the risks they face. Popular perceptions that the campus is dangerous could not only discourage high-caliber students from applying to Berkeley, but could further imperil public funding, a major enterprise risk and threat to the mission.

Conclusion

At UC Berkeley, the traditional risk manager and enterprise risk manager have learned that, far from rivals, they are allies in the effort to control campus risk. Exposure to enterprise risk management makes the traditional risk manager more strategically savvy. Exposure to traditional risk management makes the enterprise risk manager more operationally savvy. By borrowing freely from each other and coordinating efforts, they increase their individual effectiveness and maximize the likelihood of reducing their campus's overall risk.

About the Authors

Andy Goldblatt has been the risk manager at the University of California, Berkeley, since September 2011. He was assistant risk manager from 2007 to 2011 and litigation coordinator from 2003 to 2007. His areas of specialty include litigation, administrative policy, travel, and student risk. Prior to entering the risk arena, he earned a meager income as a freelance writer.

Hans Gude joined the staff of the University of California, Berkeley, in 2008, as manager, controls and accountability in the Office of the Controller. In 2011 he transitioned to the newly created position of director, enterprise risk services, in the Office of Ethics, Risk, and Compliance Services, responsible for implementing ERM on campus. Before joining UC, Berkeley, Hans was a director in the consulting arm of a Big Four public accounting firm, responsible for delivering Sarbanes–Oxley and other risk and compliance services to clients in the United States and Latin America. He holds professional certifications as a Certified Internal Auditor (CIA) and Associate in Risk Management, ERM designation (ARM-E). Hans holds a BA degree in philosophy and an MBA degree in finance.

Endnotes

[1] —According to "The State of Enterprise Risk Management at Colleges and Universities Today," published by the Association of Governing Boards and United Educators in 2009, only 7.1 percent of chief risk officers have primary responsibility for enterprise risk management. "http://agb.org/sites/agb.org/files/u3/AGBUE_FINAL.pdf," p. 23, retrieved on December 1, 2014.

Faced with the choice between changing one's mind and proving that there is no need to do so, almost everyone gets busy on the proof.

—John Kenneth Galbraith (1908-2006),
Canadian-American Economist and Diplomat

Anticipate the difficult by managing the easy.

—Lao Tzu (571-531 BC),

Chinese Philosopher and Poet

Choosing the Right Tools for Managing Environmental and Enterprise Risk

Howard N. Apsan, Ph.D., The City University of New York

Introduction

When The City University of New York (CUNY) issued its first university-wide risk management guide in 2008, it included the quotation often attributed to Wayne Gretzky, "Skate to where the puck is going to be, not where it has been."[1] Because few risk managers are clairvoyant—and fewer still have The Great One's predictive skills—we need effective management tools to help minimize risk. But how do institutions choose the right tools for complex organizational tasks like environmental management or risk management?

The late Aaron Wildavsky, one of the preeminent scholars of bureaucracy and a Brooklyn College graduate, taught us that most organizational decisions are incremental.[2] How CUNY selected its tools, first for environmental health and safety and then for risk management and business continuity, supports his argument. Incrementalism, a theory developed by Charles Lindblom and subsequently applied to the policy arena by Wildavsky, suggests a trial and error approach to decision making.[3] CUNY has been deliberative in selecting the tools for managing and mitigating risk, tries to use each incident as a learning experience, and recognizes that there are no finished products, just works in progress.

Although most tools start off shiny and full of promise, the tools themselves do not guarantee success.

Anyone who has visited Home Depot, or any other do-it-yourself emporium, knows that tool choices seem virtually limitless until you start to focus on the project at hand. If the work is carpentry, you don't need a trowel; if it's plumbing, you don't need a hammer—unless the project isn't going well. And although most tools start off shiny and full of promise, the tools themselves do not guarantee success.

The same concept applies to management tools. For environmental management, those tools might include EPA protocols, ASTM E50 guidance, ISO 14000 standards, and an array of proprietary strategic environmental management and TQEM systems. For risk management, they might include FEMA protocols, ISO 31000 standards, and a range of customized enterprise risk management, emergency preparedness, and business continuity systems. CUNY's Office of Environmental, Health, Safety and Risk Management has explored many of the tools available to address its environmental and risk management needs, and has implemented aspects of several. In the process, CUNY learned a number of hard-earned lessons: there are no shortcuts; one size does not fit all; and, sometimes, you just have to go back to the drawing board.

The balance of this article will try to tell the story of how CUNY learned these lessons, which may seem like aphorisms that we should have all learned early in life but didn't, and how the university is using these teachable moments to improve the process of selecting new tools. In particular, CUNY, like many other universities, is thinking of incorporating the concepts of ISO 31000 into its risk management practices, and this article will conclude with a discussion of some of the considerations involved in determining whether that's where we think the puck will be.

Environmental, Health, Safety and Risk Management at CUNY

CUNY was established in 1847 as the Free Academy by Townsend Harris whose self-proclaimed mission was to "let the children of the rich and the poor take their seats together and know of no distinction save that of industry, good conduct, and intellect."[4] Although a man of great vision, it is hard to imagine that even Townsend Harris could have pictured the evolution of the Free Academy into today's CUNY, which is the country's largest urban university system and the third largest university system in the United States. In 2015 it has 24 colleges, graduate

schools, and professional schools; serves approximately 520,000 matriculated and non-matriculated students;[5] has almost 44,000 full- and part-time faculty and staff;[6] and has more than 26 million square feet of space in approximately 300 buildings located throughout New York City's five boroughs.[7] Even more impressive are the generations of former students (like Wildavsky) that have passed through CUNY's halls, including 13 Nobel Prize winners, two secretaries of state, a Supreme Court justice, and the only basketball team to have won the National Collegiate Athletic Association and NCAA National Invitation Tournament championships in the same year.[8] And while it is likely that Townsend Harris would have acknowledged the need for chemical safety and fire prevention in CUNY's earliest laboratories, it seems that he left specific guidance about environmental and risk management to his successors.

Environmental Management

Traditionally, most university systems hold local campuses responsible for environmental and risk management. This has always been true at CUNY and remains so today. Nevertheless, in 2003 CUNY recognized the need for a central environmental health and safety function to set standards and hold campuses accountable to meet them. This was done in part to raise environmental awareness throughout the university and in part to ensure system-wide compliance as CUNY entered into a five-year audit and disclosure agreement with the United States Environmental Protection Agency.[9]

Because CUNY was one of the first public universities to participate in the EPA initiative, there was a bit of a learning curve for both parties. CUNY had to adjust to the rigors of an intensive compliance auditing regimen and the EPA had to adjust to a collaborative alternative to traditional regulatory enforcement. Nevertheless, "the EPA initiative provided the impetus for organizational learning and improvement. At one level, it forced the university to commit to compliance; at a deeper level, it made environmental management an integral part of the CUNY culture."[10]

Continual Improvement

By the end of the five-year CUNY-EPA agreement, both sides met their commitments and, I suspect, both sides were pleased when the program concluded. Nevertheless, it would be understandable for a visitor to think mistakenly that the EPA audit and disclosure agreement is still in effect: CUNY continues to audit all of its campuses on a triennial cycle, although the audit findings are no longer shared with EPA; the content of the environmental audit is largely indistinguishable from what was submitted to EPA except that we have added a health and safety component; the CUNY-wide Environmental Health and Safety Council, which was established to provide an opportunity for the EH&S officers and staff from all of CUNY's campuses to exchange information and share lessons learned, still meets on the second Thursday of every month; and the New York Campus Environmental Resource (NYCER) consortium meets quarterly instead of every other month, but now we have more than 80 colleges, universities, and teaching hospitals on the quarterly invitation list.

The outcome of the program that may ultimately be most valuable, however, is the CUNY environmental management system (EMS). Following Peter Drucker's maxim, "What gets measured gets done,"[11] CUNY collects and analyzes data from every audit to promote continual improvement. In addition to the regulatory modules included in every audit, there is an EMS module that tells us how much a campus has improved since its last audit.

Measuring Success

CUNY needed a comprehensive EMS that could link environmental health and safety indicators with general management indicators, and because of its growing acceptance, we also wanted to base our EMS on an ISO 14000 standard framework. ISO 14000 refers to a series of related standards.[12] Within the series, there are a number of components that were most germane to CUNY's audit program: ISO 14001 provided the general framework for an environmental management system; ISO 14004 provided more specific guidance for developing the EMS; and ISO 14031 provides a system for environmental performance evaluation.[13]

For some organizations, ISO 14000 certification is needed because of stakeholder, customer, or other extrinsic demand. For CUNY ISO 14000's premise that environmental impact can be measured and improved

was sufficient; the added cost and other obligations of certification were therefore unnecessary. And although ISO 14000 does not provide explicit performance targets, CUNY's audit criteria already establish a performance standard of full compliance. As such, the University was able to draw from another university's EMS—with permission and attribution— and tailor it to CUNY's specific needs. Seven years later, albeit with periodic review and amendment, that EMS serves as CUNY's basic environmental management tool.

Lessons Learned

The process provided CUNY with several teachable moments, underscoring the aphorisms mentioned above:

There are no shortcuts. If you think that simply drafting an EMS means that you have an effective management system, you are probably being overly optimistic. CUNY's EMS is a standard operating procedure that provides general guidance and direction. Its implementation, however, has evolved over years and is still a work in progress. Furthermore, continual improvement is an elusive target. It may sound intuitive, but there is seldom unanimity in its definition, and in many cases, people do make the same mistakes more than once.

Continual improvement is an elusive target. It may sound intuitive, but there is seldom unanimity in its definition, and in many cases, people do make the same mistakes more than once.

One size does not fit all. Neither ISO 14000 nor any other EMS comes designed for the specifics of your institution. The aspect/impact analysis and the targets and objectives have to be painstakingly tailored to each organization or they will be of limited utility. When CUNY applied another university's EMS to its operations, it assumed that most of the adjustments would require little more than editing. It turned out that process needed much more managerial elbow grease than originally anticipated.

Sometimes, you just have to go back to the drawing board. ASTM guidelines, ISO standards, and most proprietary systems are updated periodically to adjust to changing circumstance. In fact, if you are reluctant to revisit your own systems because of the cost or disruption, you may find that those changing circumstances have rendered parts of your EMS obsolete.

Systems like ISO 14000—and in the CUNY case, systems derivative of ISO 14000—enable organizations to address environmental metrics strategically. Failing to do so results in reactive behavior and exacerbates risk. In a university as large and complex as CUNY, crises and emergencies are unavoidable, but they have to be the exception rather than the rule.

Risk Management

As the CUNY risk management website states: *The City University of New York is committed to ensuring a comprehensive risk management program to reduce liability in all areas of university activity. EHSRM is responsible for organizing and implementing a program to enable the university to fulfill the objectives of risk management. One example of this effort is the development of a university-wide risk management council composed of delegates from each campus and other members of CUNY administration. The CUNY risk management program addresses a number of key risks including: emergency response plans, training programs, hurricane preparedness, business continuity, accident prevention, and regulatory compliance.*[14]

In reality, as was noted in a 2008 *URMIA Journal* article, CUNY's risk management and business continuity efforts are designed to be collaborative and to foster consultation. Day-to-day coordination, however, falls to CUNY's Office of Environmental, Health, Safety and Risk Management. This includes leadership of the CUNY Risk Management and Business Continuity Council—and coordination of its monthly meetings; chairing the monthly Emergency Preparedness Task Force meetings; conducting annual risk surveys, developing updated risk maps, and periodically revising the CUNY risk management plan; preparing emergency-specific continuity of operations plans; and maintaining the university's risk management, business continuity, and emergency preparedness

website. It also involves coordinating all of these activities with stakeholders throughout the university and with external agencies and organizations.

Continual Improvement

All of these risk management responsibilities are tracked and analyzed to ensure that the university is doing its utmost to minimize risk. An illustrative example of CUNY's commitment to continual improvement is the Emergency Preparedness Task Force. The task force, which consists of senior CUNY executives, meets every month to review significant incidents that occurred during the previous month. Much like the NYPD's CompStat, those involved in the incident meet with the task force to go over the details of the event: how it happened; what lessons have been learned; and what recurrence prevention measures have been instituted.[15] Although it is sometimes challenging, it does promote risk management collaboration and fosters a commitment to continual improvement.

Measuring Success

In many respects, tracking the success of CUNY's risk management program has been more challenging than measuring outcomes of the environmental program. For the latter, CUNY's audits and ISO 14000-derived EMS provide data on the university's progress, campus by campus. It cannot tell us how cost-effective our program is or how much was saved in fine and penalty avoidance, but it can tell us whether we are in compliance and, by the same measure, whether we are continually improving.

Since its inception, CUNY risk management has been exploring various measurement tools. CUNY's risk mapping, for example, is a composite of a number of risk mapping tools that we considered. We consulted with several enterprise risk management experts to get a better understanding of the options that might meet our strategic needs. Additionally, we reviewed risk management systems being used by other universities—both public and private—and received many helpful suggestions.

In many respects, tracking the success of CUNY's risk management program has been more challenging than measuring outcomes of the environmental program.

For our continuity of operations templates, we also reviewed a number of well-established commercial products and evaluated a number of systems that other universities had implemented. We were especially impressed by how open our colleagues were to sharing. In fact, when most universities considered developing H1N1 pandemic flu protocols, it seemed that almost all university plans were modeled after two universities' continuity of operations plans—one public, one private.

Lessons Learned

Perhaps they only become teachable moments if you actually learn from them. CUNY did learn valuable lessons from its experience with environmental management systems and applied many of them to its risk management efforts. And although environmental and risk management systems are different, the rules discussed above still seem to apply.

There are no shortcuts. CUNY was acknowledged for its work during Hurricane Sandy, especially for its management of numerous evacuation and special medical needs shelters.[16] We appreciated the kudos, but we understood that our success was attributable to the application of lessons learned from Hurricane Irene and other emergencies. Similarly, we like to think that our risk assessments get better each year because we learn from prior mistakes—poring over last year's risk maps to try to find out what we might have missed and trying to make the next round of surveys clearer and more precise as a result. It's a time-consuming and sometimes humbling process, but to paraphrase Gary Player, the harder we work, the luckier we get.[17]

One size does not fit all. When David fought Goliath, he declined Saul's weapons and armor in favor of a slingshot because he felt that it was a better fit for him.[18] When we started to look at risk management systems that were implemented at other universities, we kept thinking that a number of these systems might work at CUNY as well. Of course, as we began to drill down a bit, we realized that each university has a different risk management

system because each university is unique. And within CUNY we must always be concerned with finding tools that can be integrated well at all of our colleges.

Sometimes, you just have to go back to the drawing board. Ever since Peters and Waterman wrote their classic *In Search of Excellence*, managers have been taught to have a "bias for action."[19] In fact so many of our "quality-oriented" management systems embrace the pithy Deming "plan, do, check, act" cycle.[20] In our laboratories, scientists and engineers understand that failure is an essential part of scientific advance. Managers and stakeholders also expect action and initiative but may be less tolerant of experimentation because they are often under pressure to show results. When CUNY prepares a continuity of operations plan—hopefully well before the emergency arrives—it expects feedback from those who must rely on it, both before and after it has been implemented.

As noted, management systems enable organizations to address metrics strategically. And that brings us to the question that many university risk management leaders have been asking: what added value can ISO 31000 bring to a university's risk management program?

The Case for ISO 31000

ISO 31000, like ISO 14000, is one of numerous management standards published by the Swiss-based International Standards Organization to establish consistent, measurable global practices.[21] Process-oriented management standards like ISO 31000 are different from more traditional, product-oriented ISO standards, which were designed so that parts or products could be manufactured to consistent specifications, regardless of country of origin. The classic example is camera film—at least for those of us who remember what that is. If you are vacationing abroad and run out of film, you may rest assured that the ISO 200 replacement film that you buy in Barcelona or Beijing will generate the same quality photo as the ISO 200 film you bought in Brooklyn. It wasn't until the introduction of management standards such as the ISO 9000 Quality Standard in 1987 that ISO began to gain acceptance as a process management tool.

In the introduction to ISO 31000, the standard sets forth some basic assumptions: *Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is 'risk.'*

All activities of an organization involve risk. Organizations manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria.

Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This international standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this international standard establishes a number of principles that need to be satisfied to make risk management effective. This international standard recommends that organizations develop, implement, and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values, and culture.[22]

For CUNY these assumptions are certainly applicable, but they need some additional clarification. First, the concept of uncertainty deserves further qualification. A burst municipal water main near a CUNY building is more random than uncertain because there is no way that the university could have anticipated which main would give way or what its impact on CUNY would be. On the other hand, the impact of a hurricane on a waterfront campus is always uncertain, but the fact that it was making its way north from the Caribbean was known well in advance, as was the fact that the campus abuts the shore. These are not "distinctions without a difference" because they are key to how we map (i.e., how we identify, analyze, and treat) our risks.[23]

Further, the standard assumes that stakeholders will be engaged in a collaborative process. This plays to the strong suit of universities, which generally embrace the concept. But as most experienced risk managers know, risk tolerance varies widely, and setting uniform, measurable criteria is a substantial challenge. Beyond that, introducing a multi-faceted management system into a large, complex organization is an undertaking.

So how do we make it less daunting? ISO 31000 seems to have anticipated the question and argues that the organizational benefits far outweigh the costs of

implementation. It claims that ISO 31000 will: *Increase the likelihood of achieving objectives; encourage proactive management; be aware of the need to identify and treat risk throughout the organization; improve the identification of opportunities and threats; comply with relevant legal and regulatory requirements and international norms; improve mandatory and voluntary reporting; improve governance; improve stakeholder confidence and trust; establish a reliable basis for decision making and planning; improve controls; effectively allocate and use resources for risk treatment; improve operational effectiveness and efficiency; enhance health and safety performance, as well as environmental protection; improve loss prevention and incident management; minimize losses; improve organizational learning; and improve organizational resilience.*[24]

For CUNY, as for any large university, this list of anticipated advantages makes a compelling argument, but before we accept the notion that ISO 31000 will solve all of our problems, it may be prudent to start with a more basic question: Which problems we are trying to solve? Are we currently falling short on organizational objectives; are we not encouraging proactive management; are we failing to identify risks? And we can continue down the list.

If we think that our organization's risk management program is perfect, we should probably get a second opinion, perhaps by someone a bit less subjective. Likewise, if we know that we have problems with some or all of these items and expect that a management system alone can fix them, we will probably be disappointed. ISO 31000 is a management tool with very versatile applications, but it cannot be expected to solve long-established structural or operational problems.

So let's take a more focused look at our expectations of any risk management systems. Should it be able to improve organizational effectiveness writ large, or is minimizing an organizational risk sufficient? To try to answer this question, ISO 31000 provides a foundational list of 11 principles: *(1) Risk management creates and protects value. (2) Risk management is an integral part of the organizational procedure. (3) Risk management is part of decision making. (4) Risk management explicitly addresses uncertainty. (5) Risk management is systematic, structured and timely. (6) Risk management is based on the best available information. (7) Risk management is tailored. (8) Risk management takes human and cultural factors into account. (9) Risk management is transparent and inclusive. (10) Risk management is dynamic, iterative and responsive to change. (11) Risk management facilitates continual improvement and enhancement of the organization.*[25]

Once again, the standard may present some ambitious expectations for system-wide improvement, but at least it begins to construct a framework. At CUNY, for example, risk management has become an integral part of organizational procedure and decision making. As such, risk management activities bridge many of the silos or other bureaucratic barriers that can impinge upon organizational effectiveness. Infectious diseases, hurricanes, blackouts, and other university-wide threats do not respect bureaucratic boundaries—and they provide CUNY with unique opportunities for collaboration across divisions.

Finally, although ISO 31000 does not embrace the term, it does conclude with an informative (i.e., non-binding) annex that it refers to as "Attributes of Enhanced Risk Management." These five attributes summarize the philosophical approach of ISO 31000 in terms that would be recognizable to anyone engaged in or seriously contemplating Enterprise Risk Management.

Continual Improvement

An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review, and the subsequent modification of processes, systems, resources, capability, and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.[26]

Performance measurement is critical to continual improvement because you have to be able to quantify progress. Serious managers don't speak of impressionistic results; they want to see the numbers. Before CompStat, which we discussed above, NYPD commanders would deploy officers based on a range of criteria, qualitative and

empirical; CompStat got them to rely on statistics. Criminologist may differ on why homicides dropped steadily from 2,262 in 1990 to 328 in 2014, but every homicide has been plotted so that commanders can see clearly where they are concentrated and respond accordingly.[27] It stands to reason that an effective risk measurement system could yield improved performance as well.

Full Accountability for Risks

Enhanced risk management includes comprehensive, fully defined, and fully accepted accountability for risks, controls, and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled, and have adequate resources to check controls, monitor risks, improve controls, and communicate effectively about risks and their management to external and internal stakeholders.

This can be indicated by all members of an organization being fully aware of the risks, controls, and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases, or information systems. The definition of risk management roles, accountabilities, and responsibilities should be part of all the organization's induction programs.

The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources, and skills sufficient to assume their accountabilities.[28]

Enhanced risk management includes comprehensive, fully defined, and fully accepted accountability for risks, controls, and risk treatment tasks.

CUNY works closely with the NYPD on a range of emergency-preparedness issues—often with senior commanders and chiefs. If the subject of CompStat comes up, there is a perceptible chill in the room because anyone who has gone through a CompStat session at One Police Plaza rarely forgets the experience. If nothing else, they learned about devolving authority and accountability: a commanding officer holds all subordinates accountable for their actions because the commander will be called to task by his or her superiors.

At CUNY we are also committed to full accountability, but a university is not a police department: Its hierarchical structure is different; many employees— faculty members and administrators—have tenure or some equivalent; and academic freedom is a core university principle. So while the concept of full accountability is hard to argue with, it is not always easy to enforce.

Application of Risk Management in All Decision Making

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects, and on restructuring and organizational changes.[29]

CUNY encourages every decision maker in the university to consider potential risk. The monthly Risk Management and Business Continuity Council meetings have broad and diverse representation, and the discussions and training presentations are cross-cutting as well. A rational decision maker will always consider risk, but that doesn't mean that he or she will know all the applicable risks or understand them well enough to factor them in effectively. In Graham Allison's *Essence of Decision*, the classic study of decision making during the Cuban Missile Crisis, we learned that even President Kennedy had to make enormously fateful decisions with an incomplete understanding of the inherent risks.[30]

Continual Communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process,

such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.[31]

In an article written in 2000, "Running in Nonconcentric Circles: Why Environmental Management Isn't Being Integrated into Business Management,"[32] I borrowed the answer from a classic organization theory typology. In *Public Administration* by Herbert Simon, Donald Smithburg, and Victor Thompson, the authors include a discussion of seven traditional barriers to communication in large organizations: language, frame of reference, status distance, geographical distance, self-protection of the initiator, pressure of other work, and deliberate restrictions.[33] They were true then and they still are.

Perhaps if they were writing the book today and focusing on universities, the conclusions might have to be modified. Communication may be a prized skill in higher education, but communicating risk—especially in public universities—may be muted because of political or budgetary concerns. Again, ISO 31000 presents us with an appropriate target, but one that may be elusive.

Full Integration in the Organization's Governance Structure

Risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives.

This is indicated by managers' language and important written materials in the organization using the term "uncertainty" in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.[34]

At CUNY, risk management was established through a Board of Trustees resolution. It does not use the exact language of ISO 31000, and it does not specify a verification regime, but it does commit the university to system-wide risk management.

Effective July 1, 2007, CUNY's Office of Environmental Health and Safety expanded to become the Office of Environmental Health, Safety and Risk Management.

'Risk management' encompasses policies and procedures designed to prevent or minimize the adverse effects of incidents that may impact a campus or its related entities. Such incidents may arise from the action—or inaction—of CUNY or its officers or employees and may result in personal injury, property damage, financial loss, reputation impairment, regulatory non- compliance, or criminal liability. It is therefore incumbent on CUNY—and on each of its campuses—to manage programs and activities in a manner that controls or alleviates risk.[35]

And although the Board did not provide guidance on the selection of specific tools, it did demonstrate some foresight: "The university anticipates developing these tools and structures over the next several years as well as implementing new instruments as they may become available and relevant."[36]

Conclusion

In the lab we learn that correlation does not imply causation. Brightly colored risk maps may correlate with reduced incidence of high-impact incidents, but that doesn't mean that bright colors reduce risk (yellow caution tape and reflective vests notwithstanding). To extend the analogy, ISO 31000 doesn't reduce risk; critical thought, diligent effort, pain-staking implementation, and a forthright commitment to continual improvement are what reduce it. That doesn't mean that risk mapping and ISO 31000 won't help, it just means that they are among the tools that may be used to foster an effective risk management program.

On Wall Street, they say that past performance is no guarantee of future results. That CUNY used ISO 14000 to inform its environmental management system—without actually certifying to the standard—might suggest a similar risk management arrangement with ISO 31000. On the other hand, environmental regulations, which set definitive, auditable performance targets (i.e., 100 percent compliance), provide a backstop for the process-oriented ISO 14000; there is no equivalent for ISO 31000. Still, if past is not prologue, it can at least provide some lessons learned.

There are no shortcuts. If you're still reading, you probably know this already. ISO 14000 is a complex management system, and ISO 31000 is at least as complex. Even the graphics, which are designed to help simplify risk concepts, are very involved. Beyond that, the training is extensive, and at CUNY we have to do it 24 times.

One size does not fit all. Both ISO 14000 and ISO 31000 are designed to apply to large, complex organizations. The language of both standards makes that clear. But as they say, the devil is in the details. For any management system to work, it has to address the idiosyncrasies of the entire organization as well as its subdivisions. And, as in the case of CUNY's EMS and risk management plans, it has to be updated periodically to meet changing conditions and must consider specific campus needs.

Sometimes, you just have to go back to the drawing board. At CUNY, we do so at the conclusion of each environmental audit and after receiving each campuses annual risk management plan. We like to blame this obsessive behavior on our commitment to continual improvement, but, in reality, I think we're just afraid to offer inadequate guidance to our campuses.

If you were hoping that this article would end with a definitive statement on ISO 31000, I would suggest that you stop reading this article and find a copy of Wildavsky instead. He will remind you that large organizations, such as universities, seldom make grand, dramatic decisions. Rather, their decision making is almost always incremental. So if you want to know what CUNY plans to do next with its environmental and risk management systems, we can skate together to where the puck is going to be.

About the Author

Howard Apsan serves as the university director of the Office of Environmental, Health, Safety, and Risk Management (EHSRM) for The City University of New York, the largest urban university system in the United States. CUNY has 24 colleges, graduate schools, and professional schools; approximately 520,000 matriculated and non-matriculated students; 44,000 faculty members and other employees; and more than 26 million square feet of space in almost 300 buildings located throughout New York City's five boroughs. The university director of EHSRM is responsible for environmental health and safety (EH&S) management and compliance throughout the university; and serves as the university's risk manager, tasked with assessing liabilities and designing systems for minimizing CUNY's operational and reputational risks and promoting resiliency and continuity of operations. He also chairs the university's Environmental Health and Safety Council, the Risk Management and Business Continuity Council, and the Emergency Preparedness Task Force.

Before joining CUNY, he worked as an analyst, manager, and consultant for most of his career. He served for several years in New York City government at the Mayor's Office, the Board of Education, and the Sanitation Department. He left municipal government to pursue a career in environmental and risk management consulting, which included eight years as a principal, and ultimately national director, of a nation-wide consulting firm, and led to the founding of his own firm, Apsan Consulting, Inc. He has served industrial, commercial, and real estate clients throughout the United States and has extensive international experience.

In addition to his management and consulting activities, he has been a member of the faculty at Columbia University's School of International and Public Affairs since 1986, and also teaches in Columbia's Sustainability Management program. He is a LEED Accredited Professional and has served on the United States Technical Advisory Group (US TAG) for ISO 14000, the American Society for Testing and Materials (ASTM) Environmental Committee (E-50), and the Environmental Commission in Springfield (New Jersey)—where he is also a lieutenant in the police reserve. He chaired the New York Chamber of Commerce Environment and Energy Committee and the New York Chapter of the Environmental Auditing Roundtable and was the president of a community-based non-profit corporation. He is a member of the Editorial Board of Environmental Quality Management and writes and lectures regularly.

He earned his B.A. and M.A. from Brooklyn College, and his M.Phil. and Ph.D. from Columbia University.

Endnotes

[1] One does not become "The Great One" by taking credit for other people's quotations. Gretsky regularly attributes the saying to his father.

[2] Aaron Wildavsky, *The Politics of the Budgetary Process*, (Boston: Little, Brown, 1964).

[3] Charles E. Lindblom, "The Science of Muddling Through," *Public Administration Review*, Spring, 1959.

[4] The City University of New York. "History of CUNY," ://www.cuny.edu/about/history.html.

[5] The City University of New York. "About CUNY," http://www.cuny.edu/about.html.

[6] The City University of New York Office of Human Resources Management. "Staff Facts: Fall 2014," http://www1.cuny.edu/sites/onboard/wp-content/uploads/sites/4/Fall-2014-Staff-Facts.pdf.

[7] The City University of New York. "Facilities Planning, Construction, and Management," http://www.cuny.edu/about/administration/offices/fpcm/critical-maintenance.html.

[8] The Nobel laureates are listed at http://www.cuny.edu/about/alumni-students-faculty/alumni/nobel-laureates.html. Secretary of State Colin Powell graduated from CCNY; Secretary of State Henry Kissinger attended CCNY but was drafted into military service during WWII and graduated from another university after returning. Justice Felix Frankfurter graduated from CCNY. The CCNY Beavers won both national basketball tournaments in 1950.

[9] United States Environmental Protection Agency, *Multi-facility Audit Agreement between the Environmental Protection Agency and the City University of New York*, January 24, 2003. More information on EPA's Voluntary Audit Policy is available at http://www.epa.gov/region02/capp/cip/ and the website for the Colleges and Universities Initiative is http://www.epa.gov/region02/p2/college/.

[10] Howard N. Apsan, "The Environmental Protection Agency College and University Initiative: The City University of New York Response," *Environmental Quality Management*, Winter 2003.

[11] Howard N. Apsan, "What Gets Measured Gets Done: Two Years into the CUNY-EPA Audit Agreement," *Environmental Quality Management*, Autumn 2005.

[12] Howard N. Apsan, "ISO 14000: Setting Global Environmental Management Standards," *Metal Finishing*, August 1995.

[13] Howard N. Apsan, "Environmental Performance Evaluation: The ISO 14000 Scorecard," *Total Quality Environmental Management*, Winter 1995.

[14] The City University of New York. "Environmental, Health, Safety and Risk Management," http://www.cuny.edu/risk.

[15] For an overview of CompStat's origins and implementation at the NYPD, see John Buntin, "Assertive Policing, Plummeting Crime: The NYPD Takes on Crime in New York City," Harvard University, Kennedy School of Government Case Program C16-99-1530.0 (1999).

[16] Howard N. Apsan, "Resiliency and Continuity: Hurricane Sandy and the City University of New York," *Environmental Quality Management*, Winter 2013.

[17] Whether he originated the axiom "the harder I work, the luckier I get" is debated, but there are few harder working and luckier golfers.

[18] I Samuel, 17:38-40.

[19] Tom Peters and Robert H. Waterman, Jr., *In Search of Excellence: Lessons from America's Best-Run Companies* (New York: Harper Collins, 1982).

[20] Named for W. Edwards Deming, a leading practitioner statistical quality control.

[21] ISO 31000:2009(E), *Risk Management—Principles and Guidelines* (Geneva: International Standards Organization, 2009).

[22] Ibid., p. v.

[23] For a discussion of the distinctions between "luck, uncertainty, randomness, incompleteness of information, and fortuitous occurrences," see Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007), pp. 319-321.

[24] Ibid., pp. v-vi.

[25] Ibid., pp. 7-8.

[26] Ibid., p. 22.

[27] New York City Police Department, "Crime Prevention and Crime Statistics," http://www.nyc.gov/html/nypd/html/crime_prevention/crime_statistics.shtml.

[28] ISO 31000:2009(E), p. 22.

[29] Ibid., p. 23.

[30] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Little Brown, 1971).

[31] ISO 31000:2009(E), p. 23.

[32] Howard N. Apsan, "Running in Nonconcentric Circles: Why Environmental Management Isn't Being Integrated into Business Management," *Environmental Quality Management*, Summer 2000.

[33] Herbert Simon, Donald Smithburg and Victor Thompson, *Public Administration* (New York: Alfred A. Knopf, 1950).

[34] ISO 31000:2009(E), p. 23.

[35] The City University of New York, Board of Trustees Minutes of Proceedings, June 23, 2008, Appendix D, p. 347.

[36] Ibid.

Risk is the factor of a strategem measured by what man is powerless to control.

—Mike Norton,

American Author and Blogger

Complexity is the enemy of transparency.

—Henry Paulson,

American Banker and Former US Secretary of the Treasury

Building a Proactive Compliance Program in Higher Education

Nedra Abbruzzese-Werling and Joseph Storch, State University of New York

Introduction

Complying with the myriad legal requirements colleges and universities are subject to on a day-to-day basis is not an easy task. Similarly, creating an enterprise-wide compliance program to systematically tackle compliance obligations of a college or university cannot be accomplished overnight. However, a thoughtful and carefully planned effort for a compliance program can bring any institution into better overall compliance. This article is intended to help college and university officials in developing and implementing plans for compliance programs. While the positive results that come from implementing a compliance program may not be immediately noticed, it will only be a matter of time before your institution starts to directly see and feel the benefits of a centralized, more systematic approach to compliance.

Defining Compliance

At the outset, we need to define what the term "compliance" actually means. Within higher education, institutions must comply with a myriad of laws and rules. This is not just limited to federal and state laws and regulations. Compliance for a higher education institution also means following relevant case law and accreditation standards as well as an institution's own internal rules, policies and procedures, and even contractual obligations of the institution as a result of agreements codified into business contracts, employment contracts, and collective bargaining agreements if the institution is in a unionized environment.

Additionally, although the term compliance has a very specific meaning in the context of higher education, there is a definition of a "compliance program" that is generally accepted across all industries and is not limited to higher education. The definition comes from the *Federal Sentencing Guidelines* (hereinafter *Guidelines*), a publication of the United States Sentencing Commission. While the original intent of Congress in creating the *Guidelines* was to develop a "fair sentencing system" with more consistency and uniformity,[1] a portion of the *Guidelines* on what constitutes an "effective compliance and ethics program" has become the blueprint for the elements that a compliance program should encompass. Within the *Guidelines*, a "compliance and ethics program" is defined as "a program designed to prevent and detect criminal conduct" that consists of seven key elements. The elements, commonly referred to in the compliance industry as the "seven elements," are the minimum elements needed to form an effective compliance program.[2]

Originally for the limited purpose of reducing sentencing for bad corporate action, the *Federal Sentencing Guidelines* have now become synonymous with the elements of an effective compliance program.

These seven elements are: (1) standards and procedures—defined as "standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct;" (2) organizational leadership and culture; reasonable efforts to exclude bad actors from managerial ranks; (3) training and education; (4) monitoring, auditing, and evaluation of program effectiveness; (5) performance incentives and disciplinary measures; (6) appropriate remedial action; and (7) risk assessment.[3]

The original intent of these seven elements was to help provide a framework for federal judges who were determining culpability of a corporation that was convicted of wrongdoing under the premise that the more robust a compliance and ethics program, the less severe the corporation's punishment should be, given their efforts to follow the rules. While these elements were originally for the limited purpose of reducing sentencing for bad corporate action at the punishment phase, they have now become

synonymous with the elements of an effective compliance program across all industries.

Since the *Guidelines* first introduced the idea of an effective compliance program in 2004, the idea that an industry could and should be rewarded for having an established compliance process has proliferated into the higher education context. On an anecdotal level, various institutions have noticed that oversight agencies seem to be more lenient when the institution can show a formalized process to address compliance. Formally, this idea was recently codified into a federal task force report specifically commissioned to evaluate the federal regulation of colleges and universities. The report was commissioned by a bipartisan group of U.S. senators who formed a task force of college and university presidents and chancellors to identify potential improvements within federal higher education regulation.[4] The task force recommended that colleges and universities that have created a process for effective oversight should enjoy clear safe harbors and have good-faith efforts acknowledged. The recommendation to create a compliance program to handle laws, regulations, and policies is not new to higher education, but perhaps the formality of the task force report illustrated that the idea is gaining more traction even among policy makers. The task force only reaffirmed in a public way what higher education officials have been saying for years, especially institutions that have implemented robust compliance programs and have seen the benefits firsthand.

Growing Compliance Obligations

The overall growth of compliance obligations in higher education has been well documented. Even as other industries have seen de-regulation,[5] the *Regulation Task Force Report* confirms the growth of higher education compliance obligations by commenting on the expansion of the federal regulations—as just one source of compliance obligations—where between 1970 and 2014 the *Code of Federal Regulations* more than tripled in sheer page volume from 55,000 pages to 175,000 pages.[6] By way of actual percentage, from 1997 to 2012 the number of federal requirements higher educations must abide by grew by 56 percent.[7]

Federal research funding for higher education has increased by billions of dollars annually since programs began in the late 1940's.[8] Alongside this additional funding comes an increase in the financial burdens being placed upon colleges and universities as a result of compliance requirements–institutions responding to a survey estimated that their average costs for compliance, based upon employee hours, has risen from $66,528 in 2011-2012, to $95,568 in 2013-2014.[9] Institutions spend 26.1 million hours annually completing Department of Education mandates, and this statistic only includes the actual complying, not the development and implementation of compliance policies, processes, and guidance at the institutions.[10] The bipartisan task force report concluded in their findings that "compliance with regulations is inordinately costly."[11] Even with the additional compliance costs, research funding is likely still a decent trade-off when compared with the federal support for higher education.[12]

It has been acknowledged in recent years that "colleges and universities today are probably the most heavily regulated organizations in the United States in terms of the number and types of statutes and judicial precedents with which they must comply."[13] The *Higher Education Act of 1965* provides a good example. The law was initially passed in 1965 and was 52 pages. It grew through its eight reauthorizations and in 2008 weighed in at 432 pages. The current proposed reauthorization is about 785 pages and counting. Trying to comply with the myriad existing laws is difficult enough, but Congress, regulators, and states add new requirements each year. Beyond laws and regulations, there is also sub-regulatory guidance, letters, handbooks, opinions, and advisories issued by oversight agencies. These are just some of the sources of compliance from outside an organization and do not take into account an institution's own internal policies, procedures, and contractual obligations. Given the immensity and perplexity of the higher education compliance landscape, the question that many institutions have been grappling with is simply, "where does one even begin?"

The Rise of the Formal Compliance Function

From Reactive to Proactive – The Shift in How Higher Education Approaches Compliance and Risk

For many years, the trend in higher education was to be reactive, primarily when it came to specific national incidents—to respond after a devastating, worst-case scenario occurrence made the national headlines. There are many

examples of this reactionary approach in recent years. In 2008 the Virginia Tech shooting tragedy—and the questions being asked in the aftermath about campus safety—led institutions to develop emergency management protocols for their campuses, including notice procedures to better protect the safety of campuses in potential situations of danger. The federal government followed with their own reform to the *Family Educational Rights and Privacy Act of 1974* (FERPA) to ensure that student privacy laws did not impede an institution from alerting their campuses when a dangerous situation arose, and Congress amended the *Higher Education Act of 1965*[14] to require "emergency notifications" in certain situations.[15]

It happened again in 2010 with a death of a research assistant in a science lab in California. The incident was attributed to inadequate safety protocols, and criminal charges were filed against both the University of California Board of Regents (the governing oversight body for the University of California system of campuses) and the professor who had ultimate supervisory duties. Suddenly, institutions across the country were working to ensure proper safety protocols in their labs and adequate training so that those working in the labs were following the industry standards for safety protocols.

In 2012 it was the Pennsylvania State University child sex abuse scandal that led many institutions to develop child protection policies and protocols—and even led to increased athletics oversight and reporting changes—given the implication that inadequate oversight and institutional control of Penn State's athletics programs could have contributed to the failed reporting and investigation of the incidents of abuse on Penn State's campus. Many state governments followed suit as well, enacting mandatory reporting laws and other restrictions and protocols to govern child protection in higher education.

Most recently, 2014 was marked by an intensified national and political focus on sexual assault and Title IX, following a handful of articles published in various national news sources that began to question campus safety and institutional responses to sexual assault occurring on and around college campuses. This focus has led to institutions across the country working to hire Title IX coordinators who could be solely focused on an institution's Title IX efforts. It also led to the federal government enacting significant regulatory reforms that expanded higher education's compliance obligations regarding sexual violence and crime reporting.[16]

Ebola was another crisis of 2014 whereby a handful of Ebola cases in the United States led institutions to assemble leadership groups to enact protections and ensure their institutions prepared for any outbreaks; they were also ready to follow the latest Centers for Disease Control protocols should they experience a scare in their region.

For many years, the trend in higher education was to be reactive—to respond after a devastating, worst-case scenario occurrence made the national headlines.

With each of these issues, higher education institutions scrambled to respond—with increased lab safety focus, with child safety protocols, and with increased attention to the *Clery Act*, Title IX, and Ebola by institutions large and small. The federal and state governments also reacted with legal and regulatory reforms that significantly expanded the compliance obligations of colleges and universities. The trend is to be reactionary—to scramble in the midst of a crisis that gains national attention.

The alternative to this reactionary approach is one of proactivity—to have a system in place for addressing a crisis, whether national or specific to the institution, prior to any major incident arising. This proactivity is manifesting itself in the form of compliance and enterprise risk management programs at institutions. The concept of these programs is to create a structure around all compliance obligations and risks so that institutions proactively understand them and make efforts to mitigate them in a consistent and proactive way before a crisis arises.

Cost of Non-Compliance

It is also important to note here that the costs of compliance incidents are not just reputational. There are signifi-

cant actual costs to incidents that have occurred at various institutions. Take the previous national compliance incidents as examples.

At Penn State, the university publicly stated that the cost of the scandal regarding child abuse that was occurring on their campus was $3.2 million as of February 2012 for legal, consultant, and public relation fees.[17] That figure was released in the midst of the ongoing situation. Since that time, Penn State has fought with the NCAA to have certain team victories reinstated to the Penn State football record, and they have hired many personnel to build and cover the compliance structure that was required by the settlement agreements the institution entered into.

In California the defense of the UCLA professor—who was criminally charged for the death of the research lab assistant as a result of compliance failures that led to the injury—cost the institution $4.5 million.[18] This figure was only attributed to the professor's defense, not the costs of defending the board of regents or the expense of developing better processes and protocols at campuses as a result of the settlement agreement that was reached between the UC System and prosecutors. California, Penn State, and other compliance examples illustrate how the costs of compliance failings are actual costs that the institution must absorb.

Even compliance issues that are less prominent end up costing an institution. For example, an Office for Civil Rights (OCR) review can cost an institution hundreds of hours of personnel time, and that is before a finding is made. If a finding favors the complainant, the institution will inevitably have to devote resources—both personnel and monetary—to comply with the findings of an investigation.[19]

Even compliance issues that are less prominent end up costing an institution.

Compliance and Enterprise Risk Management Functions

Given the ever-growing landscape of compliance laws and regulations that institutions are subject to and the costs associated with non-compliance both financially and in reputational harm, a general consensus has emerged: institutions need to formalize a better process for handling their compliance obligations. The 2015 Task Force on Federal Regulation of Higher Education report concluded that "effective oversight [of compliance obligations] can help colleges and universities keep costs down, keep students safe, focus on educating students, and be good stewards of federal funds."[20]

Campuses across the country are in agreement as formal compliance offices and functions have become the norm rather than the exception. A 2013 study conducted by the National Association of College and University Attorneys[21] showed that of the responding institutions, 17 percent had a formal compliance function in place for more than three years with 14 percent having created a new function in the last three years. Twenty percent had reported having a compliance function in active development, with another 18 percent reporting that they planned to develop a program. This means that nearly 70 percent of institutions who responded had or were creating a formal compliance function. These formal compliance functions are leading to formal compliance positions. In the last 10 years, the number of employment positions in higher education with a "compliance officer" in their title has grown by 33 percent.[22] This study also only contemplates an 'officer' title, not other positions (director, vice president, etc.).

Roadmap for How to Create a Compliance Function at Your Institution

Significant value can be derived from creating an independent compliance function for your campus that seeks to be proactive in compliance efforts, including avoiding monetary loss from issues of non-compliance, preventing damage to reputation, and avoiding the demands on executive time that come with compliance crises. Institutions can prepare before an incident occurs, whether the incident is in the form of an audit, investigation, request for information, litigation, or an occurence that gains the attention of the press. It is only a matter of time before the concept of being rewarded for having a compliance process will take hold formally in the higher education world, just as it has in corporations and the medical industry. The dilemma faced by an institution that has de-

cided to create a compliance process is, "with all of these issues and requirements, where does one begin?"

Take it One Step at a Time – Eating the Enormous Elephant

There is an old joke about the problem with eating an elephant: you can't figure out where to begin. Compliance programs create a similar predicament in that there are so many requirements in so many disparate areas that it is hard to know where to start, and it is easy to throw up one's hands and save compliance for another day.

Institutions working to develop compliance programs must not get caught up in the enormity of the project. The work of a compliance office is never completely finished since laws, regulations, sub-regulatory guidance, and institutional policies will be ever-changing. In other words, the goal posts will always move. Therefore, an institution is best served if they recognize the enormity of the task, set reasonable and realistic goals for progress, and keep moving forward to effect change.

One such acknowledgment is to understand that an institution will not be able to guarantee complete compliance immediately. In fact, many in compliance agree that a full-fledged compliance program takes 3 to 5 years to become fully functional. Therefore, an institution should focus less on complete, 100 percent compliance as a goal and instead focus more on building methods, processes, and reporting structures to help departments with their own compliance. To use a sports analogy, think of the process in terms of football: if a football team does not huddle and formulate a plan prior to the start of the play, their chances of success go down. In other words, compliance will be much easier to establish when there is a plan and the university staff is working together as a team with the ultimate goal of getting the institution into compliance.

Silos Must Come Down

Just as "it takes a village to raise a child," it takes an entire campus to comply with laws and regulations. Traditionally at many colleges, some departments do not interact with one another (and some refuse to even speak) for historical, financial, or personality reasons. With all due respect to those reasons, to comply with the current panoply of legal and regulatory requirements, silos must come down.

The days are gone where a college president could assign *Clery Act* compliance to the police chief or director of security, Title IX to the athletics director, and OSHA compliance to the head of facilities and rest easy. Today's regulatory regime requires cross-campus efforts and regular meetings and interactions between staff that otherwise may never interact.

Take *Clery Act* compliance, for example. While your institution's annual security report is likely issued by campus police or security, proper compliance requires obtaining certain statistics from the conduct office, student affairs, residence life and housing, and international programs as victim notifications may come from a variety of offices. Mandatory trainings may be conducted by still other offices. Some of the law interacts with Title IX, while other aspects require interactions with local and distant law enforcement. This is not the job for a single person or even a single office. Colleges that have used such a method have paid dearly financially and in reputation when major incidents occurred. Many colleges that have cross-institutional teams that communicate regularly have prevented such incidents. It takes an entire college administration working together to comply. Reducing the effect of silos is a necessary step in developing a compliance program.

Steps to Create a Compliance Function

For most institutions developing compliance programs, the question of where to begin is daunting. As much as the beginning process will be dependent upon each institution and what they already have in place, there are a few universal steps that are good starting points for all institutions embarking on the task of creating a compliance function or structure:

1. Build a Compliance Matrix

A compliance matrix is the idea of creating a spreadsheet of all of the federal and state laws and regulations, local municipal laws, case law, accreditation standards, and all the internal institutional policies, procedures, and rules, all of which together comprise the compliance obligations for your institution. The reason a matrix is a natural first step is because before you can create a process to attempt to establish compliance for your institution, you need to first understand the universe of what exactly you must comply with.

The matrix is not only a good exercise to determine the "what," but it should also be used to identify the "who" – as in who at your institution is responsible for compliance with the specific law, regulation, policy, procedure, or rule. The "who" could be an office, a role (specific title), or a specific employee. This office/role/person is often referred to as the compliance "owner" because they own the function of satisfying a particular operational compliance function. This step of determining who owns the compliance function is important to the process of creating a matrix because it establishes accountability for particular compliance actions and also communicates to the "owner" that just because the institution is going through the process of creating a compliance function with staff members devoted to compliance, this does not mean the responsibility for completing the compliance has shifted to another person or office. The offices need to understand that they will still be responsible for "doing" compliance, but now they will have help with determining what the compliance looks like and creating a matrix whereby the office/role/person knows that they are ultimately responsible for ensuring that the compliance obligation is fulfilled.

Note that an extensive matrix already exists for all of the federal laws and regulations that apply to higher education. It is available on the Higher Education Compliance Alliance website for download (see the URMIA website at my.urmia.org for the link or check the list of resources at the end of this article). Refer to the website as the matrix is continually being updated. If your institution utilizes this matrix for your federal obligations, you should note that you need to add one more column to the chart: A column that allows you to denote who at your institution is the "owner" of the compliance function.

In 2015 the U.S. Department of Education issued its own "Compliance Calendar,"[23] but it is published as a single PDF document, is limited to certain specific compliance requirements, and is not organized in a database manner that can be searched or re-organized to best meet the needs of different institutions.

In addition to creating a matrix of resources, your institution should decide upon broader categories to bring together particular compliance obligations. The idea is to create some sort of organization to your matrix. It should be noted that sometimes compliance obligations will fit into more than one category for an institution. As an example, your institution may have a "financial compliance" category, and a "student compliance" category. Financial aid and tuition compliance obligations could fit under either of these categories. There will be inevitable overlap, just as there is overlap of duties for compliance obligations among offices at your institution. The question of which category tuition falls under is not as important as ensuring that it is included on your matrix, whatever categorization structure you choose.

A potential format for institutions to use for their own compliance matrix is available in Appendix A to this article. Since a federal matrix of laws and regulations is a resource that already exists, you should capitalize on it by using this resource to map the federal compliance obligations. Therefore, any matrix your institution creates should incorporate the already existing federal matrix in addition to local laws (state and municipal), internal policies and procedures, accreditation requirements, and any contractual obligations.

Note that an extensive matrix already exists for all of the federal laws and regulations that apply to higher education.

Once the matrix template is created, the institution will have to fill in the matrix with information specific to the institution. A good first step is to conduct interviews with the institution's functional areas. In these interviews, you will be trying to ascertain who is fulfilling specific compliance functions. Some potential questions for the interview subjects are the following: (1) What are your key compliance functions/areas of expertise/areas of involvement? (2) What laws/regulations/policies/accreditation standards must you comply with? (3) Which compliance obligations require active action on your part? (4) What resources do you rely on (internal and external) to help comply? (5) How well documented is the compliance? (6) Who documents the compliance? (7) When a compliance question comes up, who do you turn to? (8) What communication on compliance issues occurs at the institution? (9) Who

are the experts in the compliance subject area? (10) What type of compliance activity or resources would improve your area—examples include a new policy, an internal audit, guidelines, a template form, a new guidance document, more staffing, and more support from leaders. (11) What Internal Controls are in place for your area? (12) What training takes place to ensure compliance obligations are met? (13) What oversight do you have, internally and externally? (14) Who is your direct report?

All of these interview questions will help your institution to get started on determining who is doing what for compliance. When gaps in compliance responsibility are identified, this list will help you determine who would be best suited to fulfill the compliance obligation that does not yet have an "owner."

2. Define Your Compliance Program's Mission and Roles – Oversight or Resource?

Another crucial first step for an institution to determine is what the mission of the compliance function or program will be, what role it will fulfill in relation to other departments on campus, and the charge of those working for or participating in the program. This should be set and communicated at the outset of the program because a lack of mission and defined roles will result in confusion about what the program is attempting to achieve and who is going to be doing the actual compliance.

An institution will need to decide whether the compliance function will operate as a resource or as an oversight function.

To determine the mission, an institution will need to decide whether the compliance function will operate as a resource or oversight function—whether it will be set up to help or whether departments will have an obligation to report to the compliance office on their activities in a structured way. Both models have their challenges. A resource office will need to establish relationships with the offices to encourage that they are used for the office's compliance needs and issues. In contrast, an oversight office needs to be given the proper authority—and have the perception of authority from the employees—to operate effectively.

It may seem like a minor distinction, but it makes a big difference. Resource offices strike less fear in departments across the campus and colleagues believe they can ask questions openly and honestly, but ultimately, each of those stakeholders will have to affirmatively choose to take steps towards compliance. As a supervisor, one can demand that departments and professionals move into compliance quickly or immediately, but it may be a pyrrhic victory as those professionals and departments may not run all issues to ground and significant (and avoidable) problems may arise later. Ultimately, whether a resource or oversight office, or a mix, the type of compliance function an institution chooses is a policy and value judgment. The institution should think about whether they want a facilitator, advisor, and helper that inspires offices to come into compliance or whether they would prefer a supervisor that requires and tracks compliance across the institution. You should consider your current culture and whether or not a resource model or an oversight model would be best to address any compliance deficiencies.

Additionally, the institution will need to determine how many personnel they will need to devote specifically to the compliance function and what titles those personnel will have. Typically, the title of "compliance officer" denotes more of a direct oversight function, where a "compliance director" or "compliance manager" would be a coordinator with the offices and stakeholders—but there are no rules about what each title means within higher education. Compliance at each institution is not one-size-fits-all. Creating a compliance structure at your institution is about leveraging your existing structures, including audit, enterprise risk management, hotline administration, and your policy office, while creating a compliance function that monitors, communicates, and keeps track of ongoing and new institutional compliance issues. Whatever form that may take is a decision made by the institution after considering the current structure of the campus.

One concept that should be universal in creating a compliance function regardless of whether it is a resource or oversight office is clearly communicating that the com-

pliance obligations of particular offices remain unchanged. Any compliance personnel hired to support the institutional compliance function will not suddenly be doing all the complying; that would be an impossible feat given the growth of compliance obligations over the years. Instead, it should be clearly communicated that the compliance personnel are there to help with existing compliance including reviewing, monitoring, prioritizing, and keeping up with any changes, but they will not be taking on all of the compliance responsibilities.

In determining the mission, roles, and structure of a compliance program, your institution will also need to consider the following:

Who will the compliance function report to?

It is considered a best practice to have the compliance function report to high-level personnel in order to establish direct access to leadership, to establish tone at the top, and to allow for sufficient authority to the compliance function. Ideally, the compliance function would also have a direct reporting line to the institution's oversight board—to create accountability on the campus—where the compliance projects and priorities would be reported and then followed up on with reports of progress. Additionally, this direct line to the board would allow for the compliance personnel to report any instances of wrongdoing at the institution that need to be brought to the board's attention.

The most important part of compliance is building a culture where participants "do the right thing" in service of the campus community.

What is your compliance structure?

In addition to any compliance personnel hired to specifically support the compliance function, a good way to get others at the institution involved is to create a committee of higher-level administrators at the institution who oversee compliance within their areas. Membership of the committee should try to encompass all key compliance areas. This committee helps to allow for leaders around the institution to hear what other areas of the institution are doing for compliance and will help to make individual departments feel as though they are a part of the compliance effort.

3. Motivate Your Institution and Get Buy-In from the Top

We have found that the best method for compliance is to spend less time telling higher education colleagues what they are doing wrong and more time teaching them how to do things right—and even better—how to meet best practices in the field. It should be remembered that the most important part of a compliance program isn't simply the ability to check a box that you minimally meet the requirements of a law or regulation. More important is building a culture where participants "do the right thing" in service of the campus community and create an effective, safe, enjoyable space in which to learn, live, teach, research, and continually grow and improve.

4. Assess your Institutional Risks, Prioritize Projects, and Develop An Annual Compliance Plan

Your institution should use an assessment to determine the biggest compliance risks. Compliance assessments can take many forms. They can be a formal survey asking institutional leaders and employees to rank their risks or interviews asking those same personnel what "keeps them up at night;" in other words, what are their biggest compliance worries? However the assessment is conducted, an institution must assess itself in order to identify priorities.

After your risks and priorities are established, you will need to analyze what structure would best mitigate the compliance risk. This mitigation plan can come in many forms: a policy and/or procedure; additional staff/more resources; enhanced training; stronger leadership in the area; a best practices document; increased audits; or other methods to help mitigate the risk. When these projects are decided upon, they should be formally included in an annual compliance plan. This plan will become the framework for the priority compliance projects for the year. The plan should discuss the exact compliance project, the timeline goals, the personnel who are contributing, and any other considerations. The follow-up to the plan will provide a framework for any formal reporting the compliance function does, whether to the board or a high-level supervisor.

Important Considerations for your Institutional Compliance Function

Tone from the Top

The term "tone from the top" is used frequently in the compliance field. Originally an accounting principle, the idea is that an organization's ethical tone comes from its leaders and senior management. Applied to compliance, the idea is that if your leaders are saying to do the right thing and doing the right thing themselves, then that ethical tone will trickle down to the middle- and entry-level employees.

There is a story that best illustrates this principle of "tone from the top." The story, retold from other versions, goes something like this: A corporation could not determine why their employees had low morale and had trouble with following specific rules. The corporation hired consultants, who came in and evaluated the company. The senior leaders were always acting ethically and in compliance with company rules and laws, so the consultants could not figure out where this unethical "mood at the middle" was coming from until they asked the employees directly: "Why is it that the company employees do not always act ethically and follow the rules despite the tone from senior leadership?" The response was surprising: the employees watched every day as the company president pulled his car into the spot right out front labeled "No Parking." The consultants were surprised to learn that all the ethical and rule-following behavior of the senior management didn't mean a thing when the simple act of parking in a "No Parking" zone communicated to the employees that the rules didn't matter. That story is one of the best ways to illustrate just how important the tone at the top can be in determining the ethical culture of the company and that even simple acts of wrongdoing can affect employee perception in a negative way, which can impact the ethics and compliance climate of the company.

"Tone from the top" is the idea that an organization's ethical tone comes from its leaders and senior management.

Why Ethics is a Part of Compliance

Often times, the term compliance and ethics are used hand-in-hand, and many compliance programs, especially in higher education, call themselves "compliance and ethics programs." Aside from the *Federal Sentencing Guidelines* defining the seven elements of a "compliance and ethics program," there are other reasons why these terms fit naturally together. First, the idea of being compliant is similar to the premise of acting ethically—if we are ethical, we want to do the right thing because it is the right thing to do. Additionally, compliance structures are in place not only to be sure we do the actual complying but also to help us determine what is the right and compliant thing when faced with new compliance challenges. When ethics is taken out of the compliance equation, we have no incentive to be compliant as an institution. An ethical culture fosters a culture of accountability, and accountable employees are more likely to do the right things when it comes to compliance. At institutions of higher education, where colleges and universities are always striving to do better (often as a result of their underlying educational mission), it makes sense that ethics is part of the equation of a compliance program.

Use Existing Resources – Because You Aren't Reinventing the Wheel

Your campus will not be the first institution that struggles to comply with laws and regulations and you do not need to reinvent the wheel. While specific requirements and how to comply with them can differ significantly based upon your campus and its culture, there are myriad resources available to use in whole or in part to get you much of the way towards compliance:

1. Higher Education Compliance Alliance - www.higheredcompliance.org

The Higher Education Compliance Alliance is a project of several national higher education associations that collects and organizes compliance and legal resources and makes them available. The website also features a compliance matrix that can be organized by topic or by calendar, a crucial resource in not "eating the elephant" all at once.

2. URMIA - my.urmia.org

The University Risk Management and Insurance Association (publisher of this article) has a deep library available to mem-

bers and offers programming in live and online formats over the course of the year.

3. Society for Corporate Compliance and Ethics - www.corporatecompliance.org
The Society for Corporate Compliance and Ethics offers an annual conference solely on higher education issues as well as a number of annual and specialized conferences. The organization also offers members a library of resources.

4. National Association of College and University Attorneys - www.nacua.org
The National Association of College and University Attorneys offers members and their institutions resources and programming, much of it in the area of compliance.

5. SUNY Compliance Site - system.suny.edu/compliance
The SUNY Compliance Website (maintained by one of the authors) is a comprehensive site of resources on various higher education compliance issues. Resources prepared by SUNY may be freely adapted for non-commercial higher education use with attribution. A sister Office of General Counsel site with additional legal information and relevant articles is located at system.suny.edu/counsel.

6. Catholic University General Counsel - counsel.cua.edu
Similar to the SUNY site but with a longer history, the Catholic University site is well-recognized for comprehensive and well-organized resources, written by Catholic U. staff and others, that can provide information on a number of topics. The content is covered by a Creative Commons license.

Any of the above-listed resources will take a campus professional fairly far down the road of compliance, but it must be remembered that while requirements are often national or regional, best practices may differ by campus. Two colleges a few miles apart may have very different resources, programs, and cultures, and therefore may (properly) comply with requirements in very different ways. This isn't to say that a compliance officer should not start with samples and documents prepared by others, it is simply to say that while one can start there, one must not end there. Each document, policy, and procedure should be carefully tailored to meet the institutional goals, methods, and governance requirements.

Communication Is Key to a Successful Program
A compliance initiative by an institution cannot overlook a key element – effective communication. Communication is so crucial to compliance because it helps to inform your institution's personnel about your compliance efforts and simultaneously helps to create buy-in. Communication should be improved and streamlined so that people at the institution know where to find compliance information, including the institution's policies and procedures, guidance documents, forms, deadlines, and other useful information to help them with their compliance obligations.

A compliance initiative by an institution cannot overlook a key element—effective communication.

Document Your Institution's Compliance Efforts
If you are exercising stellar compliance practices every day and have a structure in place and designated responsibility but you are not documenting your efforts, it may seem like you did nothing when an oversight agency comes knocking at your door. All this is to say that you should not overlook creating documentation with any and all of the compliance efforts your institution embarks upon.

Continually Assess and Monitor
As we mentioned previously, the goal posts move in higher education compliance. That is why a critical function of any compliance program is to continually monitor and assess compliance efforts. Slight shifts in personnel and job roles can change good compliance into non-compliance. Additionally, the compliance function needs to re-assess for new issues and risks at least annually and assess the effectiveness of the compliance structures they have put in place. This re-assessment is critical to ensure the effectiveness of your efforts and because, as an institution, you cannot fix what you do not measure.

Conclusion

The creation of a compliance program or function at your higher education institution is not something that will happen overnight. It will take careful time and planning to determine how the function will operate within the existing organization and how you will define that role and communicate it to your institution. The goal is to create a function that acts as a resource or oversight for your campus' efforts regarding compliance, to help your institution proactively meet its compliance obligations, and to mitigate and help prevent compliance risks at your institution. There is no one-size-fits-all program, so institutions will have to evaluate their needs and wants when creating a compliance function that will support their institution. The ultimate goal is to create process and structure that fosters a culture of compliance at your institution so that when faced with daunting compliance challenges, as most higher education institutions are today, there is already a framework for, and resources devoted to, ensuring compliance. In the long term, any college or university that devotes resources to create a proactive compliance function will be well served.

About the Authors

Nedra Abbruzzese-Werling joined the State University of New York System Administration on March 1, 2012. Her duties are to establish, coordinate, and maintain a university-wide compliance program that tracks legislative and regulatory compliance requirements, to create and maintain a SUNY compliance website that provides information, guidance, and resources on compliance topics that impact SUNY's 64 campuses, to strengthen communication and training on compliance issues, and to identify compliance systems and experts at various campuses and levels across the university. She is also responsible for maintaining the university-wide policies and procedures web page and serves as records management officer for the SUNY system.

Ms. Abbruzzese-Werling graduated from the University of Connecticut, cum laude, and received her J.D. from the University of Connecticut School of Law. She is an admitted member of the Connecticut bar, and a Certified Compliance and Ethics Professional, a credential of the Compliance Certification Board.

Joseph Storch is an associate counsel at the SUNY Office of General Counsel and chair of its Student Affairs Practice Group. Joe has trained several thousand higher education professionals and organizations on compliance with the Clery Act, Title IX, and related obligations. In 2014 he received the Commissioner's Award from the NYS University Police, and in 2015 NACUA awarded him its First Decade Award. He graduated Summa Cum Laude from SUNY Oswego, has a Masters of public policy from the University at Albany and a law degree from Cornell Law School. After law school, he clerked for the Appellate Division, 3rd Department. His writing has appeared in the *Chronicle of Higher Education*, *Inside Higher Ed*, the *NYU Journal of Intellectual Property & Entertainment Law*, the *Albany Law Review*, the *Albany Times Union*, the *Orlando Sentinal*, *Court Review: the Journal of the American Judges Association*, the *Medical Trial Techniques Quarterly*, and he has authored seven peer-reviewed *NACUA Notes*.

Endnotes

1 *Guidelines Manual*, United States Sentencing Commission, November 1, 2014, pg. 2.

2 The seven elements of an effective compliance and ethics program are what the court is supposed to consider when determining the culpability of an organization convicted of wrongdoing. The court is supposed to review the compliance structure of the convicted corporation, and offer a reduced sentence if it finds that the company had established elements of an effective compliance program. The idea is that the corporation's punishment will be less severe if they have a set process for compliance. *Guidelines Manual*, United States Sentencing Commission, November 1, 2014. Sec.8B2.1, pg. 502.

3 *Guidelines Manual*, United States Sentencing Commission, November 1, 2014. Sec.8B2.1, pg. 502 – 505.

4 *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015.

5 Stephen Dunham, "Government Regulation of Higher Education: The Elephant in the Middle of the Room," 36 *Journal of College and University Law* 749, 750, 2010.

6 *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015, pg. 7.

7 *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015, pg. 7.

8 Dunham at 752.

9 *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015, pg. 141

10 *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on*

Federal Regulation of Higher Education, February 2015.

[11] *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015.

[12] See Dunham at 763, 783.

[13] Barbara A. Lee, "Fifty Years of Higher Education Law: Turning the Kaleidoscope," 36 *Journal of College and University Law*, 649-651, 2010.

[14] *Higher Education Opportunity Act*, Public Law 110-135.

[15] Codified at 20 USC 1092(f).

[16] See e.g. 2013 *Reauthorization of the Violence Against Women Act*, http://www.govtrack.us/congress/bills/113/s47/text; Department of Education Office for Civil Rights April 2011 Dear Colleague Letter, http://www2.ed.gov/about/offices/list/ocr/letters/colleague-201104.html.

[17] Penn State Scandal Fast Facts, CNN.com, updated Jan. 26, 2015. http://www.cnn.com/2013/10/28/us/penn-state-scandal-fast-facts/.

[18] UCLA spent $4.5 million on legal costs in Sangji case, *Chemistry World*, Oct. 20, 2014, Royal Society of Chemistry. [URL: http://www.rsc.org/chemistryworld/2014/10/ucla-spent-45-million-legal-costs-sangji-harran-case].

[19] The Office for Civil Rights of the United States Department of Education is an oversight agency of the federal government that has jurisdiction over higher education institutions with regard to Federal civil rights laws that prohibit discrimination in programs or activities that receive federal financial assistance from the Department of Education, including Title IX. Penalties for non-compliance can include an institution being deprived of the Federal funds they receive. U.S. Department of Education, Office for Civil Rights website, http://www2.ed.gov/about/offices/list/ocr/index.html.

[20] *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015, pg. 5.

[21] "2013 NACUA Compliance Survey," compiled by the National Association of College and University Attorneys.

[22] *Recalibrating Regulation of Colleges and Universities: Report of the Task Force on Federal Regulation of Higher Education*, February 2015.

[23] United States Department of Education, "Institutional Reporting and Disclosure Requirements for Federal Student Assistance Programs," http://www.nacua.org/documents/DOEComplianceCalendar.pdf

SOURCE OF COMPLIANCE: Federal Statute State Statute State Executive Order Institutional: Policy Procedure Contract Obligation Accreditation Requirement Other	CORRESPONDING REGULATION:	REPORTING REQUIREMENTS AND DEADLINES:	ADDITIONAL RESOURCES:	CAMPUS "OWNER" OF THE OPERATIONAL COMPLIANCE: Position Specific person Office
Academic Programs and Instruction				
Environmental Health and Safety/ Facilities				
Student Affairs Issues				
International Programs				
Immigration Issues				
Employee Relations				
Human Resources – recruiting and hiring, benefits, retirement, wages				
Tax and Finance				
Research				
Athletics				
Campus Affiliates/ Foundations				
Campus Safety				
Contracts and Procurement				
Accessibility/ Disability				
Diversity/ Affirmative Action				
Grants Management				
Governance				
Healthcare				
Insurance				
Information Technology, Security & Privacy				
Intellectual Property, Copyright & Technology Transfer				
Audit				
Governance				

Appendix A: One potential format for your institution's compliance matrix.

All institutions, regardless of size, must resist the temptation to under-invest in the systems and controls they need to prevent greater risk and larger losses in the future.

—Thomas J. Curry,

Lawyer and US Comptroller of Currency

URMIA Survey Shows Practices for Tracking Training Compliance

Carol Munn, CRM, CPM; Glenn Klinksiek, CPCU, ARM, MBA, DRM, URMIA

Introduction

URMIA surveyed its members in February 2015 to find out what the current practices are for tracking training and background checks in higher education. Tracking the ever-increasing number of mandatory trainings and background checks for compliance has become arduous.[1] How can you demonstrate that everyone has had the training required by law or institutional policy? The goal of this survey was to learn how colleges and universities manage compliance tracking requirements, who does the tracking, and what they track.

From the 76 survey responses, the key findings of the survey are: (1) Only 22.4 percent of responding institutions indicated satisfaction with their current tracking system while over 40 percent are in the process of implementing a new system. (2) Institutions primarily distribute responsibility for training compliance and for tracking to the departments that are responsible for compliance with the particular regulations. (3) Educational institutions use a variety of systems to track training compliance, mostly home-grown, suggesting no commercially available system has become the preferred solution to the training tracking challenge.

Demographics

Responses were fairly evenly split between public and private institutions with 48 percent (36) of the respondents from public institutions and 52 percent (39) of the respondents from private institutions. Responses were also fairly split between institutions with student full-time-equivalent populations of less than 5,000, between 5,000 -14,999, and more than 15,000.

Satisfaction with Tracking Systems

Fewer than 25 percent of respondents were satisfied with the tracking system at their institution. Of the rest, more than 40 percent are working to implement a new system. These observations held true for public and private institutions. Institutions with lower enrollments are either satisfied with their system or not working on improving them. Medium and large institutions tend to be working on new systems if they are not satisfied with their current processes.

What is your institution's approximate full time equivalent (FTE) number of students?		
Answer Options	**Response Percent**	**Response Count**
Less than 5,000	31.6%	24
5,000-9,999	18.4%	14
10,000-14,999	11.8%	9
More than 15,000	38.2%	29
answered question		76

Table 1: Full time equivalent enrollment at respondents' institutions.

Responsibility for Training Compliance and for Tracking Training

The survey sought to find out where responsibility for compliance with employee training and background check compliance rests and who is responsible for tracking training. The options for compliance responsibility are: (1) distributed: designated departments or units are responsible for training compliance in specified areas (for example, EH&S ensures employees receive OSHA required training while HR ensures all required employee background checks are performed); (2) decentralized: departments and units have the responsibility to know what training is required of their employees and to ensure that they get it; (3) centralized: one department or unit ensures compliance with most training requirements; (4) employee-centric: employees are responsible for obtaining the training they need; (5) not designated.

The survey responses indicate that nearly 60 percent

of the responsibility for ensuring training and background checks is distributed to departments with the functional responsibility in the area subject to the training requirements. Only 17 percent of responses say that responsibility for compliance is centralized.

Which statement best describes the state of training and background check tracking at your institution.		
Answer Options	**Response Percent**	**Response Count**
Our processes need improvement and we are working to implement a new system.	42.1%	32
Our processes are working satisfactorily	22.4%	17
Our processes could be better but we are not actively working to upgrade them	19.7%	15
Our processes need improvement but we are unable to identify a workable solution	10.5%	8
Do not know	5.3%	4
answered question		**76**

Table 2: Satisfaction with existing tracking processes at respondents' institutions.

Private institutions appear to have centralized responsibility for training compliance slightly more frequently than public institutions while public institutions seem to prefer distributed responsibility.

Most institutions have distributed responsibility for ensuring training compliance and none of the respondents use the employee-centric model. Smaller institutions tend to have more centralized responsibility for training compliance than larger institutions, but fewer small institutions have distributed responsibility than larger institutions.

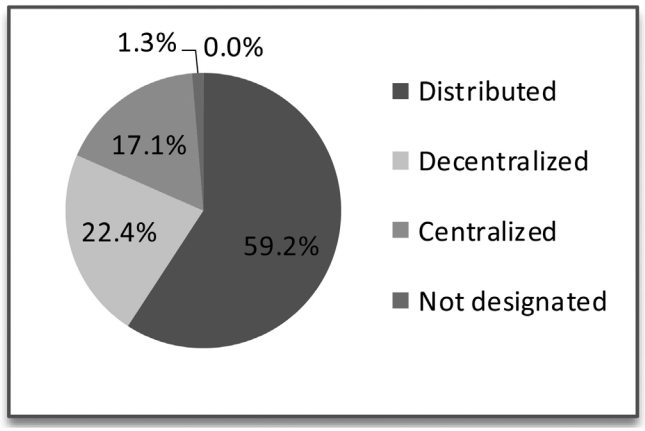


Figure 1: Responsibility for ensuring employees and others have received required employee trainings and background checks.

Answer Options	**Public**	**Private**	**All**
Distributed	63%	56%	59%
Decentralized	23%	22%	22%
Centralized	14%	20%	17%
Not designated	0%	2%	1%
Employee centric	0%	0%	0%

Table 3: Responsibility for ensuring training compliance at respondents' institutions by institution type.

As with responsibility for compliance, responsibility for tracking training and background checks can be done in five ways. The breakdown of tracking responsibility among the five possibilities shows that this responsibility is frequently distributed just as it is for compliance responsibility. However, relatively more institutions have centralized responsibility for tracking than use the decentralized approach.

Answer Options	Under 5,000	5,000 - 9,999	10,000 - 14,999	Over 15,000	All
Distributed	46%	71%	56%	66%	59%
Decentralized	21%	21%	44%	17%	22%
Centralized	33%	7%	0%	14%	17%
Not designated	0%	0%	0%	3%	1%
Employee centric	0%	0%	0%	0%	0%

Table 4: Responsibility for ensuring training compliance at respondents' institutions by FTE.

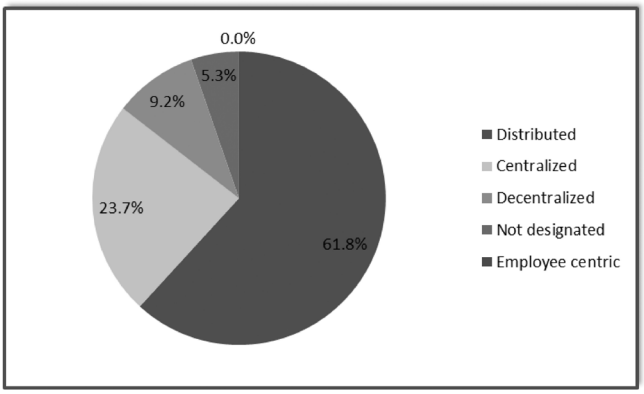


Figure 2: Responsibility for tracking required employee trainings and background checks, (that is, managing the data but not necessarily overseeing compliance).

The survey shows that three-quarters of the institutions responding to the survey place responsibility for compliance and for tracking in the same way. The 19 institutions that placed responsibility differently did so as shown in the following table.

Private institutions more frequently have centralized responsibility for tracking training than public institutions just as they did for responsibility for training compliance. Centralized tracking responsibility is more common than for training compliance. The change results from a relative decrease in decentralized responsibility for tracking responsibility.

Smaller institutions tend to have more centralized responsibility for training compliance than larger institutions, but fewer small institutions have distributed responsibility than larger institutions.

Compliance Responsibility	Differing Responsibility for Tracking		
Centralized	Distributed Tracking (1)	No Designated Tracking Responsibility (1)	
Distributed/Designated	Centralized Tracking (5)	Decentralized Tracking (1)	
Decentralized	Centralized Tracking (2)	Distributed Tracking (7)	No Designated Tracking Responsibility (2)

Table 5: Differences in tracking responsibility for centralized, distributed, and decentralized programs.

Answer Options	Public	Private	All
Distributed	61%	63%	62%
Centralized	19%	28%	24%
Decentralized	14%	5%	9%
Not designated	6%	5%	4%
Employee centric	0%	0%	0%

Table 6: Responsibility for ensuring training compliance at respondents' institutions by institution type.

Answer Options	Under 5,000	5,000 - 9,999	10,000 - 14,999	Over 15,000	All
Distributed	46%	79%	78%	62%	62%
Centralized	33%	21%	11%	21%	24%
Decentralized	13%	0%	11%	10%	9%
Not designated	8%	0%	0%	7%	5%
Employee centric	0%	0%	0%	0%	0%

Table 7: Responsibility for ensuring training compliance at respondents' institutions by FTE.

Tracking System

If responsibilities for tracking are centralized, the survey showed that human resources almost always handles the task. Legal was mentioned by two respondents while two institutions said risk management shares the responsibility with legal or human resources.

For centrally managed systems, other departments can enter training information into the central system about half the time. The table below shows how often specific departments can do so according to the survey.

If the tracking system is centralized, what other departments can enter data in the system and run reports?		
Answer Options	**Response Percent**	**Response Count**
Human Resources	60.7%	17
Risk Management	21.4%	6
Environmental Health & Safety	14.3%	4
Compliance	14.3%	4
Campus police or security	10.7%	3
Athletics	7.1%	2
Finance and accounting	7.1%	2
Legal	7.1%	2
Student Life/Activities	3.6%	1
All other departments and units	3.6%	1
Provost	0.0%	0
Deans	0.0%	0
Computing and information technology	0.0%	0
answered question		**28**

Table 8: Departments with access to training tracking at institutions with centralized tracking.

The survey responses indicate that colleges and universities use a range of systems to track training. At this point, institutions seem to use homegrown systems more often than enterprise systems.

Answer Options	**Response Percent**	**Response Count**
Excel based system	25.7%	18
Other in-house software system	21.4%	15
Other system	17.1%	12
Don't know	15.7%	11
PeopleSoft	14.3%	10
Outsourced systems capturing specific types of training	14.3%	10
Outsourced system capturing most required training	12.9%	9
Access based system	7.1%	5
We have no system	7.1%	5
Oracle	2.9%	2
SAP	1.4%	1
PowerCampus	0.0%	0
answered question		**70**

Table 9: Systems used to track training at respondents' institutions.

Other systems used by respondents include: (1) Banner; (2) Colleague; (3) Blackboard; (4) HIS-PC Compliance Training Module; (5) Absorb Learning Management System; (6) Metric Stream; (7) Sakai and My Learning; (8) Skillsoft; (9) Success Factors; (10) Webadvisor, Ellucian; (11) WeComply; (12) Workplace Answers and Student Success.

Some training generates certificates as evidence of completion. In addressing where to keep these certificates, the institutions have not settled on any particular place to keep them as shown in the chart below.

Options mentioned by respondents for certificate retention include: (1) certificates are sent to the trainees

once confirmation of completion is received; (2) completions recorded in our software; (3) vendor keeps track of completions; (4) varies depending on the nature of the training requirement; (5) learning management system generates certificates and retains electronically.

For training completions, are the trainees instructed to send their completion certificates to:		
Answer Options	**Response Percent**	**Response Count**
Designated hubs/departments	25.0%	18
Trainees keep the certificates themselves	22.2%	16
Other	22.2%	16
One central location	16.7%	12
Supervisor is responsible	13.9%	10
answered question		**72**

Table 10: How respondents' institutions track completion certificates.

Relying on vendors to track completions can be a problem if the institution changes vendors or loses access to the training data. One university reported that its training provider changed its learning management system and did not import all of the records of completed training. Consequently, the university keeps a paper record of trainees who completed training before the cut-off date.

According to the survey results, those needing training are commonly informed about the process by letter, memo, or email. Most institutions make the training process part of new-employee orientation. About 75 percent of respondents use more than one way to communicate the tracking process while 20 institutions use only one method.

Besides the methods listed in the chart, other ways to communicate the tracking process include: (1) reminders on paycheck or payroll direct deposit confirmation; (2) supervisors reinforce responsibility to ensure employees are aware of training obligations; (3) supervisors email employees.

How do you communicate the tracking process to the faculty, staff, and students?		
Answer Options	**Response Percent**	**Response Count**
Directed communication to persons needing specified training (letter, memo, email)	75.3%	55
New employee orientation	52.1%	38
Email blasts	50.7%	37
Departmental presentations	31.5%	23
Training specific webpage	23.3%	17
Department webpage	21.9%	16
Newsletters	20.5%	15
Imbed the information in the training notices	13.7%	10
Other	9.6%	7
Posters	5.5%	4
answered question		**73**

Table 11: Tools used to communicate the tracking process at respondents' institutions.

Respondents indicated no predominate way to ensure compliance. About 30 percent use management reports to show compliance, and another 30 percent have a compliance function responsible for assurance. A similar number of institutions have no method for assuring compliance.

Colleges and universities track a wide variety of training and background check requirements; the survey asked about 19 specifically. The table below shows the frequency of which the respondents said their institution tracks them. The survey did not ask why some were tracked while others were not.

Assurance training and background compliance is provided by		
Answer Options	**Response Percent**	**Response Count**
Included in department or unit management reports	31.9%	22
We have no method for assuring background training and compliance	31.9%	22
Compliance function	29.0%	20
Internal audit	15.9%	11
Legal	8.7%	6
answered question		**69**

Table 12: Training and background compliance responsibility at respondents' institutions.

Conclusion

The survey results did not identify one favored solution for managing the growing requirements for training and background check compliance. Of the public institution responders, 89 percent had FTEs over 10,000; and correspondingly, the larger institutions favored distributed and decentralized responsibility for tracking training and background check compliance. Eighty-seven percent of the private institution responders had FTEs below 9,999, and the smaller institutions were a bit more likely to have centralized systems. The possibility exists that smaller institutions are better able to centralize procedures unlike larger, more complex institutions.

The majority of the responders are in search of better procedures, which implies they have reached their tipping points with managing compliance data. Duplication of tracking efforts across departments is a problem. Providers of compliance tracking tools should find a ready market in higher education.

Please check the trainings and checks below that your school tracks.		
Answer Options	**Response Percent**	**Response Count**
Background checks	94.7%	71
Motor Vehicle Administration Driver's License checks	85.3%	64
EEO Law/Sexual Harassment training	72.0%	54
Bloodborne Pathogens training	70.7%	53
Driver Safety training	69.3%	52
Campus Sexual Violence Elimination (SaVE) Act training	68.0%	51
Research laboratory safety (general and specifically required training)	62.7%	47
Electrical Safety training	60.0%	45
Fire and life safety	60.0%	45
Teaching laboratory safety	58.7%	44
Commercial Driver's License Physicals	56.0%	42
Reporting Child Abuse on Campus training	56.0%	42
Forklift training	54.7%	41
Violence Against Women Reauthorization Act (VAWA) training	53.3%	40
Confined Space Awareness	48.0%	36

Emergency Communications training	41.3%	31
Shots Fired on Campus training	32.0%	24
Required professional continuing education units (CEU) or training to maintain licenses	32.0%	24
Act 126 Training – (3 hour course on Child Abuse)	9.3%	7
answered question		75

Table 13: Types of training and background checks tracked by respondents' institutions.

About the Authors

Carol Munn served as the director of procurement & risk management at Alvernia University in Reading, Pennsylvania, until 2015. Before joining Alvernia, Ms. Munn was a contract specialist at the IIT Research Institute in Chicago, Illinois, and prior to that she was a contract logistics intern at the National Security Agency at Fort Meade, Maryland. She has a BS in business and management from the University of Maryland, College Park, and a Master of General Administration from the University of Maryland, University College. She has earned the Certified Risk Manager and the Certified Purchasing Manager credentials.

Glenn Klinksiek headed the University of Chicago's risk management function for 25 years, retiring in 2012 as its associate vice president for risk management and audit. His responsibilities included directing the university's risk management and safety programs for the education, research, and healthcare enterprises. He managed its insurance and self-insurance programs; oversaw the university safety programs including laboratory, occupational, fire and life, vehicle, and radiation and environmental; maintained the emergency preparedness plan; managed its risk-based internal audit program; managed the compliance hotline and investigations; and staffed the university's compliance committee. Mr. Klinksiek holds a BS from the University of Wisconsin and an MBA from Indiana University.

Endnotes

[1] JJ Keller & Associates lists on its website over 200 potentially-required OSHA trainings alone (http://www.jjkeller.com/wcsstore/CVCatalogAssetStore/images/promotions/osha/OSHA-Training-Checklist.pdf). New regulations like the 2013 amendments to the *Clery Act* add training requirements (see "Bill could increase campus sexual assault regulations," the *Michigan Daily*, March 11, 2015, (http://www.michigandaily.com/news/campus-safety-and-accountability-bill).

Risk comes from not knowing what you're doing.

—Warren Buffett,

American Businessman and Philanthropist

The Response Iceberg

| *Troy Harris, Westmont College*

Abstract: The response part of emergency planning is the visible part, like the tip of an iceberg. Often when people think of planning that's all they can visualize. They figure if you have a response plan, you're set. But an effective response depends on a lot of work below the surface. An experienced emergency manager will already know this. This article simply offers a variety of ways to convey the importance of sufficient resources for the invisible work required to be really ready for major disruptions.

9-1-1, Lights, Sirens

Your school bursts onto the national scene when a big bad thing erupts. Then like all such flurries of media attention, it rapidly dissipates and the matter fades from the common consciousness. It stays that way if your response was masterfully handled. If not, though, unnecessary human pain and preventable property loss—plus the spectre of litigation—will linger for years.

You want and intend to have a great readiness program in place at your school, right? One that positions you for a swift and appropriate response. Whose support is needed to further that worthy cause? And what approach will resonate with them so that they will fund what it takes?

By looking at emergency management from a variety of perspectives, this article aims to help the higher education emergency manager toward the following: (1) Clarity that a well-conducted response is not accidental; it is made possible only by attending to its underpinnings; (2) ability to articulate that fact—in the language of those who determine priorities and allocate funding; and (3) confidence that, by applying a modest amount of thought, you can begin to pursue, and ultimately achieve, a solid—and really ready—emergency plan.

Why Bother?

To set the stage, consider what's at stake if you fail to plan well. (1) Visualize a scenario of showing up at your EOC with everyone clueless. Your mobilization will certainly be hindered if you're struggling with undirected chaos at that crucial point. (2) As a result, you'll face delays in getting medical services to injured people, or applying damage mitigations such as putting a tarp on a roof to keep things from getting wetter. (3) Consequently, you'll face higher costs in dollars, time, and good will to recover and restore order. (4) A fumbled response is a huge reputation risk in this era of instant national headlines and ubiquitous social media access. (5) Failure to be compliant with governing laws, regulations, and prevailing standards will make your faux pas much more difficult to defend when, on the last day before the statute of limitations runs, the school receives the lawsuit from someone harmed by a tardy and ineffective response. (6) Lack of acquaintance with proper documentation requirements can put reimbursement dollars at risk. According to the Federal Emergency Management Agency (FEMA) website, Tulane University was awarded $153 million after Katrina, but the Government Accountability Office (GAO) has demanded back over $80 million of it. None of us would want to get that letter.

> The Valentine's Day shooting at Northern Illinois University in 2008 was handled so effectively that NIU was universally acclaimed in the aftermath—and they ended up with no lawsuits or third-party claims. NIU took control of the situation quickly, activated their pre-arranged outside PR specialists, designated people to care for each affected family, and otherwise implemented a solid, structured response. Having confidence in the managed media communication, they were able to focus on "How can we help?" Ultimately, their broker tapped multiple lines of coverage to enable NIU to recover some $175,000 in costs. Their response to a horrific event proceeded favorably because NIU had put the right things into place before they were needed.

Icebergs and Vantages

The response part of emergency planning is all that most people can relate to when they watch the news—or for

some reason pause to anticipate a major disruption on campus. "Response" is the attention-grabbing sibling in the emergency management family.

The following examples will help illustrate why the conspicuous "response" piece cannot go it alone. We're going to look at the issue from each of seven "vantages" as several ways of articulating the need. All of them offer glimpses into what is beneath the surface, and why that vast invisible bulk matters.

Example 1 - The Visual Vantage: The Response Iceberg

Imagine your executives holding their weekly meetings on the bow of the Titanic, casually—or not at all—noticing the pretty white ice mountain up ahead. Use Figure 1 to introduce them to the simple fact that a well-managed response to inevitable disruption is dependent on far more than meets the eye. As you then elaborate further the rest of this iceberg will come into view.

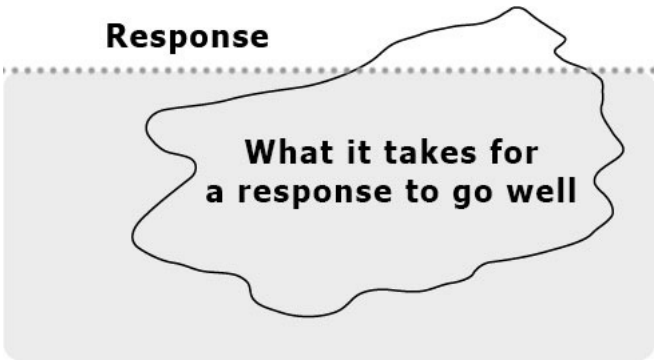


Figure 1: The response iceberg.

Example 2 - The Structural Vantage: Building Components

This view is of a building (Figure 2). Like the iceberg, there's something prominent way up high: it's a roof instead of a hunk of ice. On closer inspection you begin to realize there's also, of course, a ceiling, pillars, a floor, and a foundation.

The roof represents a timeline of action items. Ideally, we would prevent all problems in the first place. But we live in a real world. So you undertake a preparedness initiative to help care for the people in the immediate aftermath. One might also stock supplies that will help you "advance mitigate" property losses.

When the event occurs you activate your response plan. The damage mitigation team decides which roofs now need tarps on top. Even before the dust starts to settle you launch the continuity plans that each department has compiled to help them accelerate resumption of their mission. The team you've recruited to immediately commence your recovery efforts—even as the incident management team is still coping with the event itself—starts making the calls to people who will help you get back to normal. Ultimately, of course, you'll want to get reimbursed by your insurance company, by the feds, or by other sources.

Figure 2: The response structure.

In the ceiling, right under all of the activity, is the content: Methods of communicating and sending out warning messages; all the arrangements for information to flow as it must. It also includes the documentation you've put in place and the ways you've managed all the content so it's accessible to the right people at the right time. And to the right audiences certain aspects of it are published so people will know what they need to know.

The first pillar represents the people: Identifying the roles they will play; staffing each with good people; training them so they can do their jobs and ensuring they are qualified to do so; and educating your general populace.

In the practice pillar, you will perform testing and drills to build muscle memory for your responders. Assess how your exercises and even your actual responses went and maintain your gear in good shape. You'll also be mindful of ways you can incrementally refine your program keeping in mind that there comes a point when enough is enough.

The third pillar references your resources, including the entities you will work with from outside your organi-

zation or even within other parts of your institution. You need to keep good track of your materiel, facility, and financial resources. And, as Tulane learned the hard way, it can really pay off to coach your administrative and finance people in advance on how to document your loss.

Your context down on the floor includes the legal and regulatory requirements and staying current on those things. You also need to have a good handle on where you're vulnerable: a prioritized list of the hazards you face. Get clear on how long you can get by before you recover certain key resources or functions.

Finally, at the foundation of it all is the authority by which you've been commissioned to ensure your school is ready—your charter. You will have identified your scope and objectives and mustered a collaborative planning team with clear tasks and responsibilities. And woven into your plan will be such special issues as evacuation for people with access and functional needs.

Segue for a moment to the timeline aspect in Figure 3: You've got years to decades to get ready for something to come. And in the meantime you may need to repeatedly defend your planning work to those who wonder Why Bother? During the event, though, and for months to years afterward you will be thanked for your foresight.

Figure 3: Emergency response timeline.

Example 3 - The Classical Vantage: The 'W's

For generations, journalists have gotten to the heart of things by framing questions in the classic Ws. You'll immediately recognize the correlation between the previous vantage and the one in Figure 4.

Your succinct answers to these questions will educate your upline about the many invisible aspects of planning. (1) When do we need to be ready for each stage along the timeline? (2) How will people know what to do? (3) Who will be assigned to the various roles? (4) What will be done to build their "muscle memory?" (5) Where will all of your resources be placed so they're readily at hand as needed? (6) Why are we compelled to pursue all of this? (7) Which things do you tackle first? All of your planning work is the process of choosing and pursuing priorities

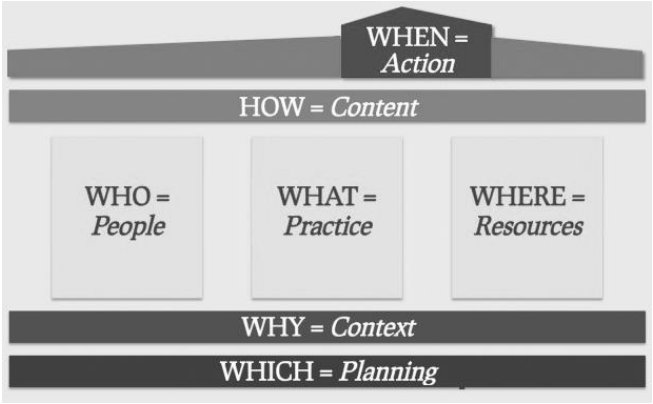


Figure 4: The who, what, where, when, why, how, and which of response.

Example 4 - The Logical Vantage: Ten Steps to Ready

There's a sensible way to structure all that's involved in getting ready for disruption. You start with nothing, and at Step 0 you get agreement on the need to have a good plan in place. Then as Figure 5 illustrates, you move through the other nine steps to encompass in your program all that the profession of emergency management has identified over several decades as being most applicable and valuable.

First, declare your commitment to being ready: (Step 0) establish your foundation.

After that you must reflect: (Step 1) Obligations: how shall I ensure we've covered our bases legally?; (Step 2) Vulnerabilities: what threats are we up against?; (Step 3) what Strategies will we implement in order to be ready for them?

The "rubber meets the road" as you address the respond concerns: (Step 4) pursue relevant Implementation activities; (Step 5) develop Competence by training the responders and educating the general public; (Step 6) ensure frictionless Communication pathways for all the information that needs to flow.

Finally, there's the review phase in which you: (Step 7) make sure the Resources are all ready to go; (Step 8) Evaluation of your capabilities by exercising your people and processes; and (Step 9) sustain a mindset of continuous Enhancement.

Where do the Ten Steps to Ready come from? As depicted in Figure 6 (and as noted in the 2012 *URMIA Journal*), at Westmont College we analyzed all the standards we could find pertaining to higher education

The Ten Steps to Ready©

	0. Foundation	We commit to getting ready.
REFLECT	1. Obligations	We will align with regulations and best practices.
	2. Impacts	We will identify our primary disruptive threats.
	3. Strategies	We will consider how to approach them.
RESPOND	4. Implementation	We will put appropriate plans into place.
	5. Competence	People will know what to do.
	6. Communication	Vital information will flow.
REVIEW	7. Resources	We will inventory our capacities.
	8. Evaluation	We will practice, practice, practice.
	9. Enhancement	We will keep getting better as time goes on.

Figure 5: The Ten Steps to Ready.

Each Plan Standard is mapped against each Framework Topic to offer a very subjective overall sense
(primarily based on wordcount) **of how much content will be found there for the practitioner to consult.**

Legend: **E**=*xtensive;* **M**=*oderate;* **B**=*rief;* **I**=*ncidental*

	Federal										Private (available at no charge)					Proprietary (available for purchase)		
Step / Topic	FEDERAL	Clery Act	FEMA CPG101:2010	FEMA HQ-EOP:2013	FEMA NPG:2011	FEMA NPS:2011	NIMS:2008	NIMS NGO:2006	OSHA 1910	PRIVATE	EMAP EMS:2013	IACLEA Blueprint:2007	NFPA 1600:2013	Red Cross Ready Rating	Resilient Orgs:2012	PROPRIETARY	ASIS SPC.1:2009	BSI 22301:2012	ISO 23320:2011
		Clery	CPG	HQEOP	NPG	NPS	NIMS	NGO	OSHA		EMAP	IACLEA	NFPA	RCRR	RO		ASIS	BSI	ISO
0. Foundation																			
0.1 Charter			B	M				B			I		M	M	B		M	E	
0.2 Scope & Objectives		B	M	E	B	B	E				B		M	M			E	E	
0.3 Plan Development				M	M			B			M		B	M	I			M	
1. Obligations																			
1.1 Requirements			M	M	B	M	E	B	I		B	B	M				B	M	B
1.2 Currency							E				B		I				I	I	
2. Impacts																			
2.1 Vulnerabilities		E	E	E	E	E					E	B	E	E	B		M	E	
2.2 Recovery Time Objectives					M								I		B			M	
3. Strategies																			
3.1 Prevention				M	E		I				M	B	M	E	B		M	M	
3.2 Advance Mitigation			B		E	M	M				M		B					B	
3.3 Preparedness				M			E						M	E	I		M	B	
3.4 Response		M	M	E	E		M		B		M		M	E	I		M	E	E
3.5 Damage Mitigation		M			M										I				
3.6 Continuity				M	M		B				B		B					E	
3.7 Recovery				M	E						B		I	M				B	
3.8 Reimbursement			M				B												
4. Implementation																			
4.1 Documents		E	B	M	M		M		I		M	B	E		B		M	M	B
4.2 Roles			M	M			E	B			M	B	M		B			M	B
4.3 Entity Relations			I	B	E		E	B			B	B	B		B			I	E
4.4 Specialty Issues				B									M					M	
4.5 Published			B	B					I			B	I		I			B	
5. Competence																			
5.1 Training				E		B	M	B	B		M	B	B	M	I		M	M	
5.2 Qualifications							E					B		I				I	
5.3 Education				E	B		I		I		B	B	I	E			M	M	
6. Communication																			
6.1 Methods			B	B	M		E	B	I		E	B	M				M	M	
6.2 Warnings		M			M		B				I	M	I					M	
6.3 Information			B	B	E		E	B			M		M		I			M	B
7. Resources																			
7.1 Staffing					B		B								B		B	B	M
7.2 Materiel				M			E	B	I				M	B	B		B	B	
7.3 Facility					B		M				B		B		I			B	
7.4 Financial				B									I		I		B	B	
8. Evaluation																			
8.1 Content Management			B	E			B		I		M	B	M		B		B	E	
8.2 Testing & Drills		B		B		B	I	B			I		M	M			B	M	
8.3 Assessment & Maintenance			B	E				B			M		M	B	M		E	E	B
9. Enhancement																			
9.1 Refinement			I	E		B	I				B		M				B	M	
9.2 Sufficiency															I			I	

Figure 6: Analysis of higher education emergency management standards.

emergency management, and organized their content by theme. We included eight federal standards and five private standards.

Thanks to the spade work of the 2007 Sloan Foundation interdisciplinary team, and in collaboration with the Standards Committee of the University & College Caucus within the International Association of Emergency Managers, we observed that the content of the standards coalesced around 10 distinct logical themes. At Westmont we eventually came to refer to these as the "Ten Steps to Ready," and as we dug deeper we began to see subthemes under each. These comprise the 35 separate topics you'll see in that matrix under the shaded bands for each step.

By allocating each of some 600 standards elements to their respective topics, we were able to create an unprecedented panoramic view of the standards landscape. As Figure 6 reveals, no topic is addressed by every standard, and more importantly, no standard—even the most robust of them—addresses all the topics. Only by blending all of that rich content in this way can one be sure everything of consequence has been taken into account.

Example 5 - The Sequential Vantage: Preponderance

Google definition of preponderance: "the quality of being greater in quantity [and presumably thus] importance." When the emergency management practitioner makes the case for developing a high-quality emergency plan, s/he can point out that they will work first on the things that matter most. How does one decide where to begin?

A prudent starting point is to address those about which more of the experts have had more to say, as reflected in Figure 7, which shows the topics listed in order by how much is said about them in the standards. We did a little math to yield this sequence (4 x Extensive + 3 x Moderate, and so on).

While everything in the standards is there for a good

Each Plan Standard is mapped against each Framework Topic to offer a very subjective overall sense (primarily based on wordcount) of how much content will be found there for the practitioner to consult.

Legend: E=*xtensive;* M=*oderate;* B=*rief;* I=*ncidental*

		Federal									Private (available at no charge)					Proprietary (available for purchase)			
	Topic / Priority	FEDERAL	Clery Act	FEMA CPG101:2010	FEMA HQ-EOP:2013	FEMA NPG:2011	FEMA NPS:2011	NIMS:2008	NIMS NGO:2006	OSHA 1910	PRIVATE	EMAP EMS:2013	IACLEA Blueprint:2007	NFPA 1600:2013	Red Cross Ready Rating	Resilient Orgs:2012	PROPRIETARY	ASIS SPC.1:2009	BSI 22301:2012	ISO 23320:2011	
Seq	* Bronze interspersed		Clery	CPG	HQEOP	NPG	NPS	NIMS	NGO	OSHA		EMAP	IACLEA	NFPA	RCRR	RO		ASIS	BSI	ISO	Math
1	2.1 Vulnerabilities		E	E	E	E	E					E	B	E	E	B		M	E		53
2	* 3.4 Response		M	M	E	E		M		B		M		M	E	I		M	E	E	51
3	4.1 Documents		E	B	M	M		M		I		M	B	E		B		M	M	B	45
4	* 1.1 Requirements			M	M	B	M	E	B	I		B	B	M				B	M	B	42
5	* 0.2 Scope & Objectives		B	M	E	B	B	E				B		M	M			E	E		42
6	* 5.1 Training				E		B	M	B	B		M	B	B	M	I		M	M		40
7	* 6.1 Methods			B	B	M		E	B	I		E	B	M				M	M		38
8	3.1 Prevention				M	E		I				M	B	M	E	B		M	M		36
9	8.3 Assessment			B	E				B			M		M	B	M		E	E	B	36
10	4.3 Entity Relations			I	B	E		E	B			B	B	B		B			I	E	35
11	4.2 Roles			M	M			E	B			M	B	M		B			M	B	35
12	6.3 Information			B	B	E		E	B			M		M		I			M	B	34
13	* 8.1 Content Management			B	E			B		I		M	B	M		B		B	E		33
14	5.3 Education				E	B		I		I		B	B	I	E			M	M		31
15	* 0.1 Charter			B	M				B			I		M	M	B		M	E		30
16	* 8.2 Testing & Drills		B		B		B	I	B			I		M	M			B	M		29
17	7.2 Materiel				M			E	B	I				M	B	B		B	B		28
18	0.3 Plan Development				M	M			B			M		B	M	I			M		27
19	3.2 Advance Mitigation			B		E	M	M				M		B					B		25
20	3.3 Preparedness				M			E						M	E	I		M	B		25
21	9.1 Refinement			I	E		B	I				B		M				B	M		24
35	9.2 Sufficiency															I			I		3
22	* 6.2 Warnings		M			M		B				I	M	I					M		22
23	3.6 Continuity				M	M		B				B		B					E		21
24	3.7 Recovery				M	E						B		I	M				B		20
25	* 4.5 Published			B	B					I			B	I		I			B		17
26	7.3 Facility					B		M				B		B		I			B		17
27	* 7.1 Staffing					B		B								B		B	B	M	16
28	2.2 Recovery Time Objectives					M								I	B	B			M		15
29	1.2 Currency							E				B		I				I	I		12
30	5.2 Qualifications							E					B		I				I		11
31	7.4 Financial				B									I		I		B	B		11
32	4.4 Specialty Issues				B									M					M		10
33	3.5 Damage Mitigation		M			M										I					10
34	3.8 Reimbursement			M				B													7

Figure 7: Analysis of higher education emergency management standards by frequency of mention.

reason, one can presume—at least provisionally—that since eight of the standards allocate extensive commentary to "2.1 Vulnerabilities," it might be sensible to give early attention there instead of to "3.5 Damage Mitigation," about which only two standards offer moderate input.

Example 6 - The Progressive Vantage: Iteration Stages

Over time the emergency manager will proceed through iterations in the planning work making the plan better with every cycle. They will work from easy to hard—from the common to the rare—periodically revisiting each topic they've chosen to pursue. We've assigned the metals Bronze, Silver, Gold, and Platinum to convey that concept. Clearly, before pursuing voluntary standards a school must have their Clery and OSHA bases covered. These plus a few topics addressing fundamental issues that no functional plan can do without, are referred to as Bronze.

As you'll see looking again at Figure 7, the topics with compulsory or fundamental aspects are indicated as Bronze (*), and are interspersed throughout. That's so because, although "Warnings" (two thirds of the way down the page) is mandatory for schools, fairly little is yet said about that topic in the standards overall. Nevertheless, we have highlighted its importance by deeming it a Bronze-level topic. Regardless of how much the standards say about something, the law holds the trump card.

At breakpoints in the formula results we grouped the topics by metal, with the top segment as the Silver range, the next segment down as Gold, and the several at the bottom referred to as Platinum.[1] What we mean by that is that—again, based strictly on the preponderance of content in the standards, and once the bronze items are in place—those topics that a typical school should, at least, embrace represent the Silver level. Schools that want to be a cut above can aim for Gold, and those with capacity and commitment can ensure they've covered all the bases, including those in the Platinum level.

The emergency manager may want to establish their program initially by ensuring only the limited mandatory elements reflected in the Bronze topics are in place. They could then come back to these later to round out their readiness by taking advantage of the voluntary elements identified with any or all of those topics. As the case is made for funding, the ongoing and iterative nature of plan development must be accounted for in your staffing plan. You'll never have an optimal response if your plan, and your responder skillset, are not essentially complete and kept current.

Example 7 - The Actual Vantage: Getting to Work

Finally, example 7 is where you'll get down to work, building on all the input so far. Many circumstances, dynamics, and priorities will influence the placement of topics in your work queue. In your presentation you could demonstrate that you've given careful thought to your priorities to ensure that the allocated funds are well applied.

Figure 8 shows Westmont's top several next areas of focus (1 to 7…); as well as those at the bottom of the stack that, for now, are considered to be in an acceptable steady state (…29 to 35). As one example of iteration, we're not starting from scratch on "6.2 Warnings" at this point; rather, although we had previously "finished" that topic a new factor prompted us to enhance our warning program—so it's been temporarily bumped back to the top of the list.

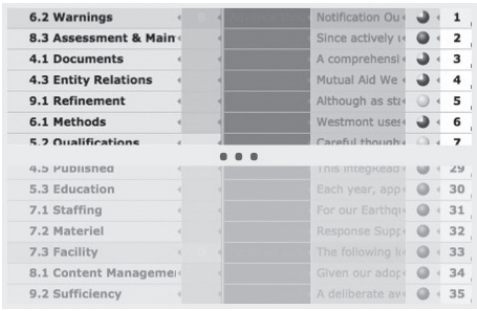


Figure 8: Westmont College sample work sequence.

Figure 9: Emergency management topics in the Ten Steps to Ready program.

Shaving the Ice

Can we make that iceberg any smaller? Figure 9 lists all 35 Topics in the "Ten Steps to Ready." Do you see anything dispensable here? Honestly, I don't. One way or another, it all has to be done if you want to manage your next major disruption with minimal pain and disruption, favorable reputation marks, and enhanced litigation defense.

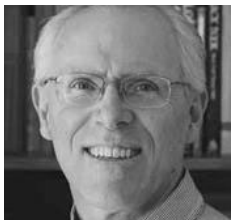
Fortunately, over a third of the work is either easy or relatively easy. Alas, some of the others will involve considerable effort. There's just no getting around it.

Articulating the Iceberg

We've talked about icebergs … and buildings, reporters, logic, preponderance, iteration, and actual. One of these images, or a combination of them, may help your upline appreciate that a superb response can only be achieved if the right elements are in place, and regularly practiced—not just sitting on a shelf!

Finally, as we like to say: "May your plans be ever better, and may you never need them!"

About the Author & Editor



Troy Harris is assistant vice president for institutional resilience at Westmont College, where they're making emergency planning easier for other schools via their íntegReady(.org) webtool, built on the Ten Steps to Ready©.

Michael Loulias is a contributing freelance editor whose rich background and varied interests include the higher education community.

Endnotes

[1] One anomaly will be observed. We exercised "artistic license" to place 9.2 Sufficiency within the silver range, because no matter what level of plan you want, you should always watch out for "plan creep."

References

The Sloan Report: http://www.sloan.org/assets/files/olsiewski/frameworkforvoluntary-preparednessfinalreport.pdf
The UCC Crosswalk: http://www.frameworked.org/crosswalk/home/
NIU event insights: John McLaughlin, Managing Director - Higher Education Practice, Arthur J. Gallagher Risk Management Services, Inc; Clair D Williams, Risk Management Coordinator, Northern Illinois University
Plan Standards - Topical: https://integready.box.com/PlanStandardsTopical
Plan Standards - Sequenced: https://integready.box.com/PlanStandardsSequenced
"Planning Pays Off" [VIDEO]: bit.ly/PlanningPaysOff

The kinds of errors that cause plane crashes are invariably errors of teamwork and communication.

—Malcolm Gladwell,

Canadian Journalist and Author

Are You Prepared to Respond to Your Next Cyber Incident?

Alan Brill and Jennifer Rothstein, Kroll Cyber Security

Introduction

It is undisputed that the advent of technology in the higher education sector has presented wonderful opportunities to students and educators alike. However, as a risk manager in that environment, you know that some of the advanced technology, if used without appropriate processes and controls, can be laden with risk. Part of your emerging role will be to support the benefits of technology while avoiding those risks. If the financial and healthcare sectors are any indicators of the likelihood of a cyber incident affecting universities, a cyber event should be characterized as a known risk; the only unknown is when will it happen and to what extent will academic pursuits be tarnished by threats of inaccessible data or, even worse, identity theft. However, experience has clearly demonstrated that those who have plans for incident response, and who have practiced table top exercises or other crisis simulations, tend to resolve them more effectively while simultaneously restoring confidence and protection to the affected individuals – a critical component for the university community.

A cyber event should be characterized as a known risk; the only unknown is when it will happen and to what extent will academic pursuits be tarnished.

Given the number of data breaches in the past year, and recognizing that the data held by post-secondary schools could be a prime target of hackers, data breaches are phenomena that demand advance planning to ensure the defensible preservation of evidence and the timely and proper notice of your carriers and constituents.

Evidence is the Key

The field of digital forensics is not always something that information technology professionals think about when preparing a response plan, but it should be. Whether an incident involves a crime—and therefore could potentially result in civil or criminal litigation—or perhaps is a violation of policies and procedures—resulting in internal administrative review—you as the risk manager may find yourself in a situation that requires you to notify your insurers of the incident. The consistent requirement for adequately informing your insurance carrier is that you need to have evidence of what happened: when it happened, who may have been involved, and whether the incident has been appropriately responded to and concluded.

Preserving evidence on digital devices is essential, because it is often subject to deliberate destruction or automatic deletion. The digital preservation process may need to include evidence stored on a smartphone, a PC in a faculty member's office, a server in the university's data center, a remote storage location connected via the Internet (e.g. cloud storage), or a local area network in a university laboratory. For example, depending on your IT policies and procedures, electronic mail messages may be automatically deleted after a time period (often 60 to 90 days). Log files may be automatically overwritten within days or weeks in the interest of saving storage space. Yet these electronic mail message and files may be absolutely vital pieces of evidence in understanding an incident.

In your experience managing all types of risk, you know that having an understanding of what happens after an incident—from the potential need to notify those whose data had been compromised to meeting the requirements of insurance contracts to dealing with the crisis communication and reputational fallout from incidents—is vital to containing the crisis and avoiding further unpredictable damage. Notably, when you receive a call in the middle of the night or over a holiday weekend—when many crises seem to occur—you do not have time to begin the planning process. You need to implement the plan.

Case Study: Cyber Crisis Management

It is six o'clock in the evening on the Friday before a three-day holiday weekend. A student taking a course in the English department wants to check the office hours of his professor in the next week. But when he opens the department's website, he sees a repeating video clip of what appears to be a dorm room and two students involved in sexual activities. The student calls the information technology help desk. The help desk immediately escalates the incident to management, and within minutes the chief information officer, communicating from a smartphone, sends an instant message to the head of computer operations. "Get that garbage off our systems NOW. If I check the site in 15 minutes and it's still there, you're gone."

The computer operations head (the chief technology officer) calls his team, and 10 minutes later the department's website is restored. The operations head sends an email to the CIO: "Website restored. We will monitor to be sure it stays fixed." A minute later a return message arrives from the CIO: "Great work. Thanks. Enjoy the rest of the holiday weekend!"

On Tuesday morning, the CIO gets a call from the general counsel. Over the weekend, someone obviously talked to the media. They not only know it occurred, but they had a copy of the video. They are demanding to know what the university is doing about the incident. The general counsel also has had a call from an attorney representing one of the students in the video and expects that a very public lawsuit alleging "revenge porn" will be filed in the next couple of weeks. The attorney also told her that the former boyfriend, Roger, is a work-study student at the school. The general counsel says that she has informed the university president and that everything associated with the incident—emails, logs, etc.—should now be considered to be covered by a litigation hold. The GC requests that all of the information be emailed to her as soon as possible and also asks for a list of everyone who was involved in any aspect of handling the incident.

The help desk immediately escalates the incident to management, and within minutes the CIO sends an instant message to the head of computer operations.

The CIO sets up a conference call with all of the information technology department managers, and it occurs within 15 minutes of the GC's call. The CIO passes along the request and schedules another call for later in the afternoon. During that call, the CIO learns that:

(1) No one is exactly sure who worked on the incident. Apparently many of the people who might have worked on it are off-duty, and one of the managers thinks one of the students in the work-study program—who assists in the data center—volunteered to help during the incident. If a student assistant did help, they would have had to use the user accounts of the full-time employees because they do not have their own administrator level accounts.

(2) There is no written report or other documentation of the incident or how it was remediated, but the operations manager says that he will try to "get the guys to put one together."

(3) The CIO reports that he spoke to a couple of the techs who worked on the response. They report that to fix the problem quickly, they just "blew away" anything they had to and re-loaded files. One of the techs says that he remembers being yelled at to fix it but not exactly what he did.

(4) The CIO also reports that the log files that could show who was accessing the server when the defacement occurred are gone – they are only held for 48 hours and are then overwritten. At this point, those logs are gone forever. Whatever external access log files are still present will be copied onto a DVD, and that will be given to the CIO.

(5) When the CIO asks that the surveillance video inside the data center be preserved, he is told that those files are also overwritten after 48 hours – the request for a larger capacity hard drive to increase the hold time to 30 days was turned down in the IT department's budget priorities last year.

(6) A quick check of the student work-study sign in/sign out log for the data center for the evening of the incident indicated that one student worker was on duty – a student named "Roger."

Right after the GC's call to the CIO, she places calls to the chief of the university's police department, the head of public affairs, and the university's risk manager. The risk manager didn't know that a problem had occurred. He calls the school's insurance broker so that the incident can be reported to the carriers involved. The broker says that he has handled cases involving cyber incidents and says that the insurer is going to tell them to secure anything they have relating to the incident. The broker also says "we may have a problem. You knew about the incident on Friday. The policy requires notifying the carrier within 48 hours. Why didn't you call me earlier?"

At the end of the day, the CTO calls the CIO and says that he's engaged a consultant to help him with the investigation and collection of evidence, and the consultant is already hard at work. The CIO calls the GC. After a few calls back and forth, the day ends with the discovery that:

(1) The "consultant" is an IT person who is a friend of the CTO. He is not a licensed private investigator (and the university's state requires "all persons who receive payment for carrying out an investigation for a third party" – including computer forensic work – to have a private investigator's license). The person also has no company, was engaged with a phone call, and is working without a statement of work.

(2) The insurer has a panel of approved forensic providers, all of whom are appropriately licensed and who are acceptable to the carrier. The "consultant" is not on the list.

This is a university that now has a lot of problems. They have very little evidence. It appears that a suspect in the incident was working in the data center and was allowed to "help" in responding. Important evidence was overwritten.

Key Planning Points

Risk managers know that inevitably risks materialize into incidents. For each there is an appropriate response, but for the incident in the case study above, the response couldn't have gone much worse.

Having a cyber incident response plan in place is a key reason cited as the difference between an effective and ineffective response. It is true that one size rarely fits all, but there are some basics to keep in mind when putting together the right response plan for your school.

First, cyber incidents cannot be considered to be simply technical events. They have legal, insurance, technical, public relations, and, potentially, law enforcement aspects. Determine how to ensure that the right people will be notified of an incident promptly and how that notification will be accomplished.

Second, determine the resources that you may need both internally and externally. You may, for example, want to limit first responders to those who have had some training in evidence preservation. You may want to appoint someone to be a log keeper to record who did what during the incident and to remind everyone working on the response that they have to log their time and activity so that you will know who did (or did not do) what.

Having a cyber incident response plan in place is a key reason cited as the difference between an effective and ineffective response.

In most cases, you will want to identify one or two outside firms that can provide forensic and investigative services. In choosing these firms, consult with your insurance carriers to determine if they have a pre-approved panel of experts. Two additional benefit of working with a pre-approved panel of experts are that typically the rates are reduced because of the panel relationship and the contracts are available to be signed even before an incident occurs. If there is no available list provided by your insurance program, interview candidate firms to be sure they understand your needs and that they comply with any licensing laws in your jurisdiction. You should then try to enter into a contract that provides for on-call services but does not obligate you for payment unless you authorize a response. Having such agreements saves valuable time during an incident because contractual requirements are already taken care of. Work with your CFO to plan for how the costs of forensic and investigative support will be handled. Even if these costs will eventually be reimbursed by insurers, you may have to bear them in the short- or medium-term.

Third, take this opportunity to review the incident reporting requirements set by the carriers and any requirements that the carrier sets as a condition for coverage –not only on the existing policy but in contemplation of a renewal policy. Sometimes, actually carrying out those requirements – and being able to demonstrate that you are doing so – falls between the cracks. Make sure that you (and your IT department) know and understand the underlying requirements set by the carriers. Discuss the process with your brokers. Some organizations work with the school's internal auditors to make the carrier requirements part of the auditor's checklists so that they will regularly check them in the course of their work.

Fourth, document your plan. Get buy-in from senior management. Executive-level managers and board members have come to understand that cyber incidents are potential time-bombs. Without proper handling, the costs of remediating these incidents can be staggering. Even if handled perfectly, costs can still be substantial; these costs are generally not budgeted, and emergency cost approval may rise to the level of senior management and the board for approval.

Fifth, as with many things—especially in the academic environment—practice is important. Many organizations hold at least an annual table-top exercise to work through simulated incidents. Are the various stakeholders ready to work together? Will your plan actually work? What if key stakeholders are on vacation or otherwise unavailable? Are there alternates ready to step in for every executive involved? Finding problems during an exercise is far better than discovering them in the middle of an actual crisis.

Reducing Cost and Impact

While the target of the attack cannot be predicted, your role as a risk manager uniquely positions you to help reduce the impact and cost of an incident by assuring that there are effective plans and resources in place. Future damage can be avoided by taking steps to preserve evidence during an existing incident. Data breaches involving student-, faculty-, or staff-sensitive information or credit card data from the bursar's office or other card-accepting organizations are the types of incidents that are probably top of mind. But there are a wide range of circumstances—from accusations of cyber bullying to misappropriation of intellectual property—where the evidence is likely to be on a computer.

Even where files or data have been erased, data can, in some cases, be forensically recovered. But this is only possible if the storage devices can be preserved or are copied using specific techniques that allow recovery to be attempted. In many cases, the reality is that you do not get a second chance to preserve the digital evidence. If you fail to get it as soon as an incident is recognized, the evidence may be gone forever. And that could include vital information, such as the proof, for example, that your incident should be covered by one of your insurance policies or that you acted appropriately to meet the post-incident requirements of a policy.

Although you are not expected to be an expert in digital evidence, hopefully knowing the importance of such evidence will help you assess if your institution has a reasonable, defensible plan for identifying, protecting, and safeguarding digital evidence. Once you have assessed the preparedness of your institution, you might consider notifying your broker of any best practices that you have implemented. Showing your carrier that you are thinking about how to respond to cyber events could afford you premium reductions or other insurance coverage benefits.

Building a Team for Digital Preparedness

In assessing your digital evidence preparedness, you should partner with your university's chief information officer and general counsel. The CIO team usually includes the first responders when an incident occurs. Immediate tasks include the determination of whether there are policies and procedures in place to prevent the inadvertent destruction of evidence in the course of immediate response actions. Horror stories abound if protocols are not followed. In prior cases we know that technical personnel took actions such as overwriting log files, reformatting disk drives believed to be infected with malware, or loading new software onto machines involved in an incident, thus potentially overwriting critical information and rendering any overwritten information unrecoverable.

While never intending to exacerbate the situation, in these instances the technicians, who were working to get the systems for which they were responsible to keep up and running, ended up destroying evidence. Maintaining digital evidence and keeping a precise log of what actions were undertaken, who did what, and what was found were just not part of the way they responded.

By working within your institution to develop a joint plan, you can improve processes, identify resources (some of which may be outside the university), and improve your outcome when an incident does hit by having a team in place that is supported by both the technology and legal units. As the cornerstone of any successful academic institution is based on collaboration amongst students, faculty, and staff, the management of cyber risk and liability should be built on a similar foundation of collaborative efforts.

About the Authors

Alan Brill is a senior managing director at Kroll. He consults with law firms and corporations on investigative issues relating to computers and digital technology, including the investigation of computer intrusions, Internet fraud, identity theft, misappropriation of intellectual property, cases of internal fraud, data theft, sabotage, and computer security projects designed to prevent such events. He has worked extensively on developing methodologies for collecting evidence from corporate information systems.

As the founder of Kroll's global high-tech investigations practice, Mr. Brill has led engagements that range from large-scale reviews of information security and cyber incidents for multibillion-dollar corporations to criminal investigations of computer intrusions. He has worked on many of Kroll's major international projects. As a part of the Kroll Experts program, he serves as both a consulting expert and testifying expert in major cases where his ability to explain complex technology concepts provides counsel with a valuable litigation resource.

Mr. Brill is an internationally recognized writer, speaker and instructor on technology security. He has authored or co-authored six books and written several articles. In addition, he has appeared on a wide range of media outlets including "60 Minutes," "Dateline NBC," "Good Morning America," *Time Magazine*, *US News & World Report*, *Wall Street Journal*, *USA Today*, NBC, CBS, and ABC News, as well as CNN, MSNBC, CNBC, BBC, A&E CBC, Discovery Networks, and Court TV. He has been an instructor for the FBI, Secret Service, Federal Law Enforcement Training Center, AICPA, ABA and the John F. Kennedy School of Government at Harvard.

Jennifer Rothstein is a director with Kroll's Cyber Security practice. She joined Kroll after a distinguished career in professional liability program management, e-discovery product development, and intellectual property ownership rights management. At Kroll Ms. Rothstein maintains and broadens the strategic partnerships established with insurance companies, brokers, and insureds. She leads cross-functional activity to facilitate new business opportunities and targeted product development as it relates to cyber liability.

Previously, Ms. Rothstein directed the development and growth of professional lines programs for business segments including lawyers, broker dealers, accountants, real estate agents, and architects and engineers. She also was co-creator of the insurance market's first e-Discovery services endorsement for over 10 lines of business for a major international carrier. She co-developed an exclusive patent liability defense program with a national broker for the tech sector's top industry leaders. Ms. Rothstein began her career in the insurance industry at AIG. In that role, she facilitated the underwriting of electronic and intangible risks into corporate insurance policies. Her role also included the enforcement of the litigation management guidelines and the review and approval of panel counsel invoices.

Cyber bullies can hide behind a mask of anonymity online and do not need direct physical access to their victims to do unimaginable harm.

—Anna Maria Chavez,

American Lawyer and CEO of Girl Scouts of the USA

Computer Security Incidents:

The Increased Threat and Implications for Higher Education

| *Christopher T. Davidson, MS, and Malcolm W. Beckett, DBA, MS, CISSP, Virginia Tech*

Abstract: Computer security incidents have increased over the past decade for both the public and private sectors, and institutions of higher education are not immune to these incidents. This article explores computer security incidents and threats for higher education campuses, discusses the implications for higher education institutions, and makes recommendations for steps that higher education officials can take to mitigate these threats and incidents.

Introduction

The number of public reported data breaches has risen during the past decade. These incidents have included virtually every industry, and higher education has been no exception. Educause demonstrates this trend with an estimated 727 higher education breaches from 2005 to 2014, with an average of 27,509 records compromised per breach.[1] In February 2015, health insurance company Anthem, Inc. announced that online attackers breached the company's information technology (IT) system and potentially obtained "the names, dates of birth, Social Security numbers, health care identification numbers, home addresses, email addresses, employment information, including income data" of 80 million customers and employees.[2] In 2012 the South Carolina Department of Revenue experienced the theft of 3.8 million Social Security numbers, 387,000 credit and debit card numbers, information for 1.9 million dependents, and 700,000 businesses.[3] Unfortunately, computer security incidents have become more prevalent over the last decade targeting businesses, the U.S. and state governments, and institutions of higher education (IHE). In 2014 the University of Maryland experienced a similar data breach affecting approximately 300,000 records.[4] Other universities experiencing data breaches in 2014 include North Dakota University, Butler University, Indiana University, and Iowa State University.[5] These types of attacks in the private and public sectors, including colleges and universities, have the potential to cost the entity millions of dollars to provide victims with credit monitoring and to repair IT infrastructure, open the door for litigation, and harm the institution's reputation.[6] For higher education administrators, it is important that IT professionals and risk managers work collaboratively to reduce the risk of financial and reputational loss by strategically aligning both facets to the mission and vision of the organization. The purpose of this article is to discuss how computer security incidents have taken place at institutions of higher education, to discuss the implications for computer security incidents and threats for college and university administrators, to make recommendations for how IT professionals and administrators can mitigate risks from computer security incidents, and how to recover from cyber incidents.

Colleges and universities are prime targets for sophisticated computer security incidents and threats because of the open and robust centers of information they house.

Computer Security Incidents and Threats on College and University Campuses

Colleges and universities are prime targets for sophisticated computer security incidents and threats because of the open and robust centers of information they house, including valuable personal information on students, faculty, and staff.[7] This personal information includes Social Security numbers, tax information, student and parent loan information, and a variety of other critical information.[8] Universities also hold intellectual property and research that could be valuable to hackers.[9] It is important to note that an institution of higher education can serve as one source of significant forms of sensitive data including personally identifiable information (PII), Health Insurance Portability and Accountability Act

(HIPAA) data, Criminal Justice Information System (CJIS) information, and restricted research. IHEs can experience as many as 100,000 or more attacks a day against campus networks primarily originating from around the world through anonymous proxy servers and other mechanisms to obscure the attacker's identity.[10]

Beyond the attempts to obtain data illegally, there are also a number of cases in which communication or media tools are defaced, including Twitter accounts like that of the U.S. Central Command and corporate and governmental websites and systems.[11] The University of Washington experienced an attack from an extremist group that took over and defaced several of the university's websites by posting text that called for the deaths of Americans in Iraq.[12] These attacks show vulnerabilities that college and university administrators must address with the use of social media and digital media.

While computer security incidents from outside sources remain an ever-growing risk for higher education administrators, human error is also a source of computer security incidents that can ultimately lead to breaches exposing an IHE to significant risk. This human error takes the form of storing PII, such as Social Security numbers, on an unencrypted mobile device that is lost or stolen. Multiple institutions of higher education have experienced these incidents and have had to provide free credit monitoring to those affected.[13] These computer security incidents have significant implications for college and university administrators.

Implications of Computer Security Incidents for College and University Administrators

Financial Implications

The most significant implication of a computer security incident and data breaches for college and university administrators are financial. In the U.S., the average cost per record for a data breach is $201. In a highly regulated field like education, the average cost per record is $294.[14] These costs can add up to hundreds of thousands of dollars or more depending on the size of the data breach. These costs can include, but are not limited to, the staff time used to address the issues through call centers, notifying victims, providing free credit monitoring services to victims, investigating the attack, and repairing infrastructure and software.[15] These costs for data breaches are not typically budgeted by college and university administrators leading officials to have to make decisions about where the money will come from to meet the institution's data breach insurance deductible or fully fund recovery activities.[16]

Reputational Implications

Data breaches at IHEs cost more than the money required to address computer security incident and data breaches. There are also reputational costs for colleges and universities. This can include having to explain and apologize for an incident to students, parents, alumni, employees, trustees, and prospective students. Since colleges and universities are constantly battling for prestige and students, administrators want the reputation of the institution to focus on being a top research university, having NCAA championships, or having top faculty experts. Colleges and universities do not want to have a reputation for being the school with data breaches. While corporations are able to quantify the loss of reputation based on a decrease in revenue after a computer security incident and data breaches, the amount of reputational cost to an IHE is harder to quantify because typically students do not leave or refuse to attend a college or university based on a history of data breaches at that institution.[17]

Legal Implications

One example of the legal risks caused by a computer security incident is the class-action lawsuit worth $6 billion against Maricopa Community College District (MCCD) in Arizona for a 2013 data breach that affected 2.4 million records.[18] In this case, the plaintiffs charged that the Federal Bureau of Investigation (FBI) was notified that MCCD's databases containing PII were posted online for sale in April of 2013 and that the community college district did not notify victims until November of 2013. The lawsuit alleges that MCCD knew of its vulnerabilities and failed to take the appropriate steps to address those vulnerabilities. The lawsuit also alleges that MCCD did not notify the victims in a timely manner and instead destroyed evidence of what information was actually taken from MCCD's systems.[19] If this class action lawsuit is successful, MMCD could spend another $6 billion on top of the $17 million it has

already spent to rectify this incident. While computer security incidents can reach into the millions of dollars in infrastructure, reputational, and legal costs, there are steps that college and university administrators can take to mitigate against these types of incidents.

Recommendations for College and University Administrators

The recent data breaches in the private sector and at colleges and universities should compel university officials to examine their IT infrastructure to mitigate against computer security incidents, data breaches, and the potential financial and legal liabilities and reputational costs.[20] College and university administrators can prevent and protect against computer security incidents by completing a holistic IT risk assessment, using mobile device management (MDM), requiring multi-factor authentication for access to university databases, and carrying data breach insurance.

Risk Assessment

College and university administrators should collaborate with IT professionals to complete a comprehensive risk assessment using the framework provided by National Institute of Standards and Technology under the U.S. Department of Commerce that includes risk framing, risk assessment, risk response, and risk monitoring.[21] During "risk framing," administrators and IT professionals work to produce a risk management strategy to identify, prioritize, respond to, and monitor risks.[22] During "risk assessment," administrators and IT professionals identify, prioritize, and estimate risks to the institution's operations, assets, individuals, and other organizations potentially affected by a security or data breach.[23] During the "responding to risk" stage, administrators and IT professionals identify, evaluate, choose, and implement the appropriate course of action to "accept, avoid, mitigate, share, or transfer risk."[24] During the "monitoring risk" stage, the final stage, administrators and IT professionals verify that there is compliance with the decisions and actions made to mitigate the risks, evaluate the effectiveness of those measures, and identify changes to the IT environment after measures have been implemented.[25]

Recent data breaches in the private sector and at colleges and universities should compel university officials to examine their IT infrastructure to mitigate against computer security incidents.

Mobile Device Management

Since the work that college and university administrators has become more mobile, another area where college and university administrators can prepare to mitigate risks is by implementing mobile device management for university business such as smartphones, tablets, and laptops.[26] To address the increased use of these devices, college and university administrators need to ensure that the data on the devices are secure as a loss or stolen device could create financial and legal risks for the university.[27] With MDM, administrators can fully encrypt mobile devices with password policies and wipe devices remotely in the event of a loss or theft.[28]

Multi-Factor Authentication

Another way that college and university administrators may be able to mitigate IT vulnerabilities is to use multi-factor authentication to access campus networks and databases.[29] Multi-factor authentication ensures that a user is who he or she claims to be when accessing campus networks and databases by requiring them to identify themselves using a combination of something the user knows such as: (a) user I.D. and password or PIN and (b) something like a security token that generates a one-time password (OTP). The IHE issues the user I.D. and password or PIN. The security token can be a small electronic device that the user physically possesses and generates a different OTP each time the power button on the device is pressed. There are also alternative methods for obtaining an OTP without the security token. These methods can include answering challenge questions online or having an OTP sent via message to a mobile device.[30] On college campuses, financial aid administrators are already using these devices

to log into the various U.S. Department of Education financial aid databases as mandated by the federal government to protect federal financial aid systems.[31] These devices could provide another layer of protection against potential exploitation of college and university databases by mirroring what the federal government's security procedures.

Data Breach Insurance

Data breach insurance is a relatively new concept; however, it is expected to grow tremendously as current general liability insurance policies that cover injury and property damage do not cover computer security incidents and risks. Therefore, it is important for college and university administrators to invest in data breach insurance. The primary difference administrators will experience with these policies is that it lacks actuarial data. Insurers will rely on the college and university's risk management program to customize a policy to cover the college or university. The college or university's operations will dictate the coverage needed and the financial cost. Data breach policies may include liability for security or privacy breaches, costs associated with data breaches like providing credit monitoring and notifications, costs of recovering from the data breach, costs related to reputational damage, and coverage for expenses related to regulatory compliance.[32]

General liability insurance policies that cover injury and property damage do not usually cover computer security incidents and risks.

For administrators seeking coverage as a means for the institution to both transfer and mitigate direct financial implications, buyers will encounter both first- and third-party insurance coverage from insurers. First-party coverage includes losses to the university's own data, lost income, or other harm to the university resulting from a data breach. Third-party coverage includes insurance against liability of the university to third parties, like students and employees, resulting from a data breach.[33]

First-Party Coverage

Types of first-party coverage may include (a) theft and fraud, (b) forensic investigation, (c) business interruption, (d) computer data loss restoration. Theft and fraud coverage includes the destruction or loss of the university's data due to a computer security incident. A forensic investigation, which is almost always warranted and often required due to regulatory requirements, covers the legal, technical, and related costs due to the exhaustive and labor-intensive investigation that may require manually analyzing logs and network traffic. Business interruption coverage covers lost income and other costs related to the college's inability to conduct business because of a data breach. Coverage for computer data loss restoration includes the physical damage to or loss of computer-related assets. These assets include retrieving or restoring data, hardware, software, or other information destroyed during a computer-security incident.[34]

Third-Party Coverage

Types of third-party coverage may include (a) litigation and regulations, (b) regulatory response, (c) notification costs, (d) crisis management and public relations, (e) credit monitoring, (f) media liability, (g) privacy liability. Coverage for litigation and regulations covers costs from civil lawsuits, settlements, and fines for incidents. Regulatory response coverage covers the legal, technical, and forensic services needed to respond to governmental inquiries, investigations, fines, and other actions taken against the university. Notification coverage reimburses the costs to notify students, employees, and other stakeholders affected by computer security incidents. Crisis management coverage includes the management and public relations costs relating to educating those affected. Credit monitoring coverage covers the cost of credit and fraud monitoring to those affected by a computer security incident. Privacy liability coverage protects against the liability to employees for a breach of privacy.

Recommendations for Purchasing Insurance Coverage

Before administrators purchase data breach insurance coverage, they should identify what their unique risks are and understand what the institution's current coverage includes. This process involves getting stakeholders

involved to assist with obtaining the right types of coverage. Once this evaluation is complete, then the administrator should purchase the most appropriate coverage for the university with the appropriate limits. When purchasing insurance, administrators should be aware of any exclusions from their coverage including acts by third-party vendors. Lastly, administrators should be completely aware of what activities trigger coverage under their policy.[35]

It is important to note here that regardless of the insurance coverage, it is impossible to mitigate the social cost and damage to the reputational damage caused by a data breach.

Conclusion

The last decade-and-a-half has seen an increase in computer security incidents and data breaches on college and university campuses. These attacks and breaches range from direct attacks from foreign and domestic hackers looking to exploit PII and research to human errors including the loss or theft of laptops that store PII. College and university administrators must work with IT professionals and college risk managers to identify and mitigate vulnerabilities in campus IT systems and infrastructure. Failing to identify and mitigate IT vulnerabilities may result in large amounts of personal records stolen, significant financial costs in the millions of dollars for colleges and universities, and a loss of institutional reputation and trust among all campus constituents.

About the Authors

Dr. Malcolm W. Beckett currently serves as the director of information technology for administrative services at Virginia Polytechnic Institute and State University. In this role, he leads the organization and technical resources supporting the division's technology needs. Dr. Beckett has a background in public service where he has worked at all levels of government, including service as a first responder. In these roles, he has led numerous cross-functional and inter-disciplinary teams where he balanced the strategic needs, operational requirements, and limitations. Much of his work has concentrated on utilizing technology to supplement and enhance business processes while providing stakeholders the tools necessary to succeed. Dr. Beckett holds a Doctorate of business administration from the National Graduate School of Quality Management, a Master of Science from Capitol College, and a Bachelor of Science from Bluefield College. In addition he holds several professional certifications including the Certified Information Systems Security Professional (CISSP) Project Management Professional (PMP) certification. He is a member of Association for Continuing Higher Education (ACHE), Institute of Electrical and Electronics Engineers (IEEE), and the American Society for Quality (ASQ).

Chris Davidson is a doctoral student in Virginia Tech's higher education program and a graduate assistant at the Virginia Tech Institute for Policy and Governance. His research interests include emergency and crisis management, Title IX of the Education Amendments of 1972, and due process, governance, leadership, and policy in higher education. He holds a B.S. in history and social sciences and a M.S. in counseling and human development from Radford University.

Endnotes

1 Educause Center for Analysis and Research, "Just in Time Research: Data Breaches in Higher Education," (2014), https://net.educause.edu/ir/library/pdf/ECP1402.pdf.

2 Anthem, "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services," (2015), http://www.anthemfacts.com.

3 Brown, Robbie, "South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere," *The New York Times*, (November 12, 2012), http://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html?_r=0 .

4 University of Maryland, "UMD Data Breach," (2014), http://www.umd.edu/datasecurity/.

5 Robin Hattersley Gray, "Top 10 Data Breaches at Educational Facilities in 2014," *Campus Safety Magazine*, (January 19, 2015), http://www.campussafetymagazine.com/article/top_10_data_breaches_at_educational_facilities_in_2014/Data_Breaches .

6 Blustain, Harvey, Janice M. Abraham, Rebecca L. Adair, Elisabeth J. Carmichael, Glenn Klinsiek, and Jane W. Thompson, "Risk Management," in *College & University Business Administration* (Washington DC: National Association of College and University Business Officers).

7 Pérez-Peña, Richard, "Universities Face a Rising Barrage of Cyberattacks," The New York Times, (July 16, 2013), http://www.nytimes.com/2013/07/17/

education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all .

[8] McDonald, Ryan, "Why the University of Maryland was ripe for a cyber attack," Baltimore Business Journal, (February 20, 2014), http://www.bizjournals.com/baltimore/blog/cyberbizblog/2014/02/why-the-university-of-maryland-was.html .

[9] Ibid.

[10] Zalaznick, Matt, "Cyberattacks on the rise in higher education," *University Business*, (2013), http://www.universitybusiness.com/article/cyberattacks-rise-higher-education.

[11] Barnes, Julian E. and Danny Yadron, "U.S. Probes Hacking of Military Twitter Accounts by Pro-Islamic State Group," *Wall Street Journal* (January 12, 2015), http://www.wsj.com/articles/u-s-investigating-apparent-hack-of-military-twitter-account-by-islamic-militants-supporters-1421086712 .

[12] Cihon, Brett, "Some University of Washington websites hacked; extremist group claims responsibility," (January 29, 2015), http://q13fox.com/2015/01/29/some-university-of-washington-websites-hacked-extremist-group-claims-responsibility/ .

[13] McCarthy, Kyle, "5 Colleges with Data Preaches Larger Than Sony's in 2014," *The Huffington Post*, (January 15, 2015), http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.

[14] Ponemon Institute, "What does a data breach cost?" (2015), http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach-risk-calculator-infographic/index.html .

[15] O'Neil, Megan, "Data Breaches Put a Dent in College's Finances as Well as Reputations," *The Chronicle of Higher Education*, (March 17, 2014), http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/.

[16] Ibid.

[17] Ibid.

[18] "G&K Attorneys File Class-Action Lawsuit Against Maricopa County Community College District for 2013 Security Breach," (2015), http://www.gknet.com/news/press-release/gk-attorneys-file-class-action-lawsuite-maricopa-county-community-college-district-2013-security-breach/ .

[19] Ibid.

[20] O'Neil, Megan, "Data Breaches."

[21] US Department of Education, "National Institute of Standards and Technology, Managing Information Security Risk: Organization, Mission, and Information System View," (2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf., 32.

[22] Ibid. 33

[23] Ibid., 37.

[24] Ibid., 41.

[25] Ibid., 45.

[26] Schwartz, Karen D., "How to Save Money, Time and Sanity with Mobile Device Management Software," *Ed Tech*, http://www.edtechmagazine.com/higher/article/2012/07/how-save-money-time-and-sanity-mobile-device-management-software .

[27] Blustain, Harvey, Janice M. Abraham, Rebecca L. Adair, Elisabeth J. Carmichael, Glenn Klinsiek, and Jane W. Thompson, "Risk Management," in *College & University Business Administration* (Washington DC: National Association of College and University Business Officers).

[28] Schwartz, Karen D., "How to Save Money."

[29] Ahubia, Mor, "Two-Factor Authentication Gaining Traction in Higher Education," *SafeNet*, (March 6, 2014), http://data-protection.safenet-inc.com/2014/03/two-factor-authentication-gaining-traction-in-higher-education/#sthash.9bynOYyz.y6YBY6rx.dpbs.

[30] Burke, Steven and James McMahon, "Two-Factor Authentication," U.S. Department of Education (2015), http://ifap.ed.gov/presentations/attachments/56TwoFactorAuthenticationV1.pdf.

[31] Ibid.

[32] "Cyber Security," National Association of Insurance Commissioners and The Center for Insurance Policy and Research, (February 15, 2015), http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

[33] "A Buyer's Guide to Cyber Insurance," (October 2, 2013), http://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[34] Ibid.

[35] Ibid.

People ask me all the time, "What keeps you up at night?" And I say, "Spicy Mexican food, weapons of mass destruction, and cyber attacks.

—Dutch Ruppersberger,

US Representative for Maryland's 2nd Congressional District

For he who has health has hope;

and he who has hope has everything.

—Owen S. Arthur,

Barbadian Politician

Are Colleges Legally Bound to Respond to Student Opioid Intoxication?

| *Joseph P. McMenamin, MD, JD, McMenamin Law Offices, PLLC*[1]

Introduction

Many college students use opioids. Some use medications of this class for the relief of pain while others use them non-medically. All medications entail risk. The most serious and important risk associated with opioid use is intentional or accidental overdose, which can result in death if intervention does not occur quickly. Given our national preoccupation with litigation, those realities justify asking whether the estate of a student dying on university property as a result of opioid intoxication could state a cause of action against that university for failing to come to his aid. Given the damage such incidents do to institutional reputation, one might also consider whether, apart from litigation risk, colleges should do more to combat the problem than most do now.

One might also consider whether, apart from litigation risk, colleges should do more to combat the problem of opioid overdose than most do now.

The Epidemiology of Opioid Intoxication

For many patients in pain, opioids are essential. Opioids include both lawful compounds such as morphine, codeine, methadone, oxycodone (OxyContin), and fentanyl (Duragesic), and prohibited ones such as heroin. Pain is now the most common reason Americans consult physicians,[2] and opioids are standard treatment for moderate to severe pain.[3] Historically, opioids were prescribed long-term mainly for cancer patients. In recent years, however, opioids are increasingly prescribed for non-cancer pain patients as well.[4]

Much of the increase in opioid use arises not among desperate street corner addicts but among patients in pain whose physicians, with the best of intentions, have legitimately prescribed them. Despite the therapeutic rationale and medical supervision, however, growing use has caused substantial harm. "Prescription drug abuse is America's fastest-growing drug problem, and one largely fed by an unlikely source—Americans' medicine cabinets."[5] According to DEA, the Drug Enforcement Administration, more than 6 million Americans misuse prescription opioids—more than those misusing all illicit drugs combined. As though in parallel, prescription opioid-related overdose deaths now outnumber overdose deaths from all illicit drugs combined.[6]

Concurrent consumption of alcohol and/or other drugs can also aggravate opioid-related risk.[7] Opioid intoxication has required higher rates of hospitalization and has caused a worrisome rise in the number of opioid-related deaths.[8] CDC estimates that 44 Americans die from prescription opioids every day.[9]

While legitimate opioid prescribing has increased substantially, illicit use has certainly not gone away. In the U.S., the number of medical emergencies involving non-medical use of opioids rose 183 percent from 2004 to 2011.[10] There were more than four times as many opioid-related fatalities in 2010 as there were in 1999, and opioid-related fatalities remained at these levels through 2013.[11] Overdoses of both lawful and illicit opioids have become the leading cause of injury death in the nation.[12] Each year, American emergency departments manage some 136,000 opioid overdoses,[13] a majority of which result in hospital admissions.[14]

Opioids and Young Adults

According to President Obama's National Drug Control Strategy, young adults aged 18 to 25 have the highest rates of current drug use at nearly 20 percent.[15] As in the population as a whole, college-age opioid users include both patients filling prescriptions and others obtaining drugs unlawfully. About 25 percent of Americans aged 18 to 20 report using prescription medications non-medically at least once in their young lives.[16] Among full-time college students aged 18 to 22, the rate of current illicit drug

use was 22.3 percent in 2013.[17] By their sophomore years, about half of all undergraduates will have been offered the opportunity to abuse a prescription drug.[18] In 2013, about one quarter of male full-time college students aged 18 to 22 were current illicit drug users (26.0 percent). Among females, the rate was lower, but at 19.2 percent,[19] still substantial. Unfortunately, among such young opioid users the level of naivete respecting overdose awareness, avoidance, and response strategies is disturbing.[20]

The Risks of Opioids

Properly used, opioids remain invaluable weapons in the fight against pain. Like all other medications, however, opioids have side effects including addiction, constipation, drowsiness, nausea, and vomiting.

A side effect that has not received enough attention is life-threatening respiratory depression.[21] The biological effects of opioids are widespread and complex, and a full discussion is beyond the scope of this article. One place where opioids work, however, is a part of the brainstem that helps generate the rhythm of respiration.[22] Opioids interfere with that function. When a patient's opioid levels reach the toxic range, breathing decreases significantly, or stops entirely, a medical emergency that can be fatal if not addressed within a few minutes.[23]

Best Practices for Overdose Prevention

Unquestionably, the best way to cope with the problem of opioid toxicity is to prevent it from occurring in the first place. As discussed below, that approach has its limits, but when prevention is feasible, its superiority over intervention is non-debatable.

American law has long criminalized the use of opioids outside a proper doctor-patient relationship. Some number of opioid-related harms have thus undoubtedly been avoided. Unfortunately, however, these laws are difficult to enforce, and, as incarceration statistics plainly show, their track record as a preventive measure leaves much to be desired.

The medical profession certainly plays a vital role in reducing risk: "Clinicians who prescribe these agents should understand the basics of safe opioid dosing, screen for mental illness in potential recipients of opioids, perform behavioral testing and urine screens to detect problematic opioid use, and use electronic prescription-drug monitoring programs…to help identify patients who may be receiving opioids inappropriately from multiple prescribers."[24]

Community-based overdose programs include education and training on how to prevent and respond to overdose.[25] A good example is Project Lazarus, established in 2008 in response to extremely high drug overdose death rates in Wake County, North Carolina. The project provides "technical assistance to create and maintain community coalitions, and help them create locally tailored drug overdose prevention programs and connect them to state and national resources."[26]

In another example, the Massachusetts Department of Public Health, the Quincy Police Department, and mental health/addiction organizations have partnered to create a program to train and equip police officers to administer an antidote to overdose victims.[27]

Community-based public health overdose prevention programs are also available in cities such as Chicago, New York, Boston, San Francisco, Philadelphia, and Pittsburgh. They train interested persons how to recognize overdoses and what to do when they occur. In as little as 20 minutes, users are trained to recognize overdoses and to respond by calling 911.[28] Although it is probably impossible to avoid opioid intoxication risk entirely, programs such as these are a step in the right direction.

Collegiate Efforts

Prevention programs are not limited to communities.

Colleges have long experience in dealing with alcohol-related problems. Their efforts to combat alcohol-associated injury and death are instructive. Substance abuse among students is not a new problem, but one that can be and is addressed by universities seeking to diminish risk:

"While the [substance abuse] problem is significant, use of SBIRT [screening, brief intervention, and referral to treatment] in campus health centers has shown promising results. Notably, a study funded by SAMHSA [Substance Abuse and Mental Health Services Administration, an agency of HHS] and conducted by the University at Albany – State University of New York found that SBIRT programs in campus health centers can help address college drinking. At a 6-week follow-up, students reported decreased alcohol use, more accurate perceptions of other students' drinking, and increased use of

strategies to enhance self-esteem and self-worth. Results of the study also indicate that changes in alcohol use were positively correlated with changes in perceptions of drinking among peers. This year, ONDCP [Office of National Drug Control Policy] in partnership with [the Department of] Education, will disseminate information on SBIRT to campus health centers and school administrators and provide university officials with screening tools and information on substance use that can be accessed on the schools' websites and in orientation materials by both parents and students."[29]

Colleges also have experience with smoking-related problems, and in some instances have succeeded in decreasing tobacco-related harms, as by implementing a smoke-free campus policy.[30]

Although it is a newer phenomenon, colleges across the nation have taken measures to prevent problems with opioid toxicity as well. In June 2014, for example, the State University of New York launched an awareness and support campaign involving all SUNY campuses, featuring educational materials and antidote training, among other measures, all designed to combat opioid abuse throughout the SUNY system.[31] Through its GenerationRx Initiative, the Ohio State College of Pharmacy has developed a multi-pronged approach, including educational programs for high school and college students and candlelight vigils to remember those who have fallen victim to prescription drug abuse and addiction.[32] The college provides training and resources for establishing collegiate recovery communities,[33] and has convened faculty members, student life staff members, students, and others from institutions of higher learning across the nation to develop strategies that participants can implement on their own campuses.[34] To curb misuse and abuse, particularly among teens, the University of Southern Nevada has created a Drug Abuse Awareness Team that along with other organizations offers area residents a venue and information for disposal of prescription and over-the-counter drugs. Unused and expired medications are collected anonymously and with no-questions-asked for safe and proper disposal.[35]

Colleges across the nation have begun taking measures to prevent problems with opioid toxicity.

Clinical Management of Opioid Toxicity

In a perfect world, there would be no need to determine how to respond to opioid toxicity, because non-patients would abstain and patients would be treated at doses high enough to relieve pain but too low to cause harm. Unfortunately, opioids have a narrow therapeutic index.[36] That is, the lethal and/or dangerous dose or concentration overlaps the effective analgesic dose.[37]

The nature of opioid intoxication is such that the victim will most likely be largely helpless. He will be obtunded and confused, if he is conscious at all. His survival may well depend on intervention by an alert bystander. Fortunately, one needn't be a physician or nurse to recognize opioid toxicity with reasonable accuracy. Opioid intoxication is characterized by some highly characteristic and fairly apparent signs: blue lips and nail beds; breathing problems or cessation of breathing; extreme sleepiness or loss of alertness; and small, "pinpoint" pupils.[38] A bystander observing such signs, and aware that the victim is on opioids, could logically infer that opioid overdose was probable and act on that knowledge. Opioid users can be trained to do this accurately.[39] SAMHSA's Opioid Prevention Toolkit[40] provides further guidance to identify candidates for antidote administration. Even more fortunate than relative ease of detection, the potential for causing harm by making a mistake in so concluding is small.

Many overdoses are witnessed by others, making intervention possible in most circumstances.[41] A student's roommates, friends, and other contacts are often those best informed about his licit or illicit drug use. On the basis of that knowledge, those persons would be the most likely not only to suspect overdose but also to be among those best-positioned to respond.

The treatment of choice in opioid intoxication is naloxone, an opioid antagonist. That is, naloxone is a medicine that interferes with the actions of opioids and reverses their effects, including life-threatening respiratory depression. Since it does not rely on oral administration, naloxone enters the blood stream rapidly. Healthcare professionals have used it for decades, saving thousands of lives.[42] Naloxone has a unique safety profile: unless the patient has taken an opioid, or is allergic to naloxone, the drug has no effect. Historically,

in fact, emergency care professionals regularly used naloxone to diagnose a suspected opioid emergency: An obtunded patient who responds most likely has opioid toxicity. Hence, naloxone is an antidote to opioid overdose, and, if administered in time, will completely, if sometimes only temporarily, reverse the effects of an opioid overdose until definitive emergency care is available.[43]

Naloxone is not a panacea: it is ineffective against benzodiazepines (Valium®, Xanax®, Klonopin®, etc.), barbiturates (Seconal®, Fiorinal®, others), stimulants (cocaine, amphetamines (including methamphetamine, Ecstasy, etc.), clonidine, amitriptyline (Elavil®), GHB, or ketamine. But its effectiveness against opioids is unequalled.

In the United States, naloxone is a prescription medication. Used primarily in the hospital setting or by EMS, injectable naloxone has been FDA-approved for more than 40 years.[44]

In April 2014, FDA approved naloxone in a new, auto-injector dosage form for use by family members, neighbors, or caregivers wherever opioids may be present, including in a home or dormitory. Using the auto-injector, a friend or bystander delivers naloxone in the outer front (anterolateral) part of the thigh, through clothing if necessary. The device provides visual and voice instructions, including directions to seek emergency medical care immediately after use.[45] Using the product requires no background in health care; it was specifically designed for lay person use. [46] Its speed of onset buys precious time for EMS providers to arrive and for more definitive management to begin.In fact, the FDA-mandated label for the drug instructs the user to inject the naloxone first, and then to call 911.

Once the squad arrives in answer to the 911 call, more definitive management can be undertaken. Further management should be left to medical professionals.

Governmental Efforts

The problem of opioid intoxication has grown sufficiently severe to merit attention from the highest levels of government. Calling the problem a "crisis," the White House has taken a very active role:

"In May 2010, President Obama released the National Drug Control Strategy, which outlined the administration's science-based public health approach to drug policy. In 2011 the strategy was expanded to place special focus on certain populations, such as service members and their families, college students, women and children, and persons in the criminal justice system."[47]

HHS has taken a number of steps to address the problem. It is increasing funding for prescription drug monitoring programs (see below), developing guidelines for opioid prescribing (through CDC), promoting expanded utilization of naloxone, expanding coverage of medication-assisted treatment ("MAT")(such as methadone maintenance programs), and coordinating the efforts of all its sub-agencies to improve the effectiveness of the overall endeavor.[48]

In 2011 the National Drug Control Strategy was expanded to place special focus on certain populations, such as service members and their families, college students, women and children, and persons in the criminal justice system.

The Department of Education has begun to address the problem as well:

"Reducing substance use behaviors among college students requires prevention strategies at the college or university as well as in the surrounding off-campus community. In response, [the Department of] Education launched an initiative in 2010 to provide a more integrated and comprehensive response to issues related to alcohol and other drug use on college campuses as well as violence among college students. This includes a new Healthy College Campuses grant program called for in the administration's fiscal year 2011 and 2012 budgets. It also includes ongoing technical assistance provided via the Higher Education Center for Alcohol, Drug Abuse, and Violence Prevention.… In addition, Education, HHS, and ONDCP are collaborating to identify and partner with university leaders to more effectively address the high rates of substance use and its consequences among college students."[49]

States are also active in taking measures to combat the

problem of opioid toxicity, especially through their prescription drug monitoring programs (PDMPs). PDMPs are databases tracking opioid prescriptions. They allow health care professionals and law enforcement to identify patients who may be at high risk. PDMPs have improved practitioners' prescribing habits and discouraged "doctor-shopping," or patients' tendency to seek opioids from a variety of prescribers to increase access to their drugs of choice.[50]

Risk for Colleges

Collegiate Negligence

Given how commonly college students use opioids, lawfully and otherwise, and given the risks associated with their use, the question arises whether a college is under a duty to recognize the risks of student opioid intoxication, and to take steps to address that risk.

With respect to potential liability for harms arising from opioid toxicity, the factor most challenging for plaintiffs is establishing that the school owes a duty of care to prevent such harms. Duty of care is the obligation to avoid injury to that individual by exercising a level of care reasonable in all the circumstances.

The extent of a university's duty to protect students from injury is difficult to capture succinctly, especially because the notion of duty changes as society does. Duty is a policy-driven, fact-specific question that depends on the particular circumstances surrounding a case. Hence, per se rules are hard to come by. Simply put, however, the negligent failure to address an identified harm—and to implement a risk management and action plan—can cause a university to be held liable for foreseeable harms inflicted on its students. Based on their history, plaintiffs' counsel, typically rewarded by a fee contingent on a recovery, will not hesitate to push the envelope through theories not yet tested.

Broadly speaking, the law recognizes no general duty of care that universities owe to prevent student injuries or to supervise their actions. This philosophy reflects the emphasis colleges place on development of their students' independence and the idea that college students are mature adults capable of responsibly regulating their own lives.[51] Hence, a student-plaintiff may face an uphill battle to prevail if his claim arises from opioid-induced harm. But sometimes uphill battles can be won.

Students successfully claiming their colleges should be legally responsible for their injuries have generally relied on either or both of two theories of liability. These theories seek to establish that the nature of the relationship between universities and their students is such as to engender a duty. Establishing such a special relationship between a university and its students, however, does not suffice. To be actionable, the injury a student suffers must have been reasonably foreseeable by the university. Foreseeability analysis asks whether the party causing the injury, or failing to prevent it, should have reasonably foreseen the general consequences that would result because of its conduct. For instance, as students regularly reside in university residence halls or other campus-provided housing, and as drug-use and drug-related injuries are relatively common on college campuses, an injured plaintiff will argue that it was reasonably foreseeable that drug use and overdose may take place either at university residence halls, at university-sponsored events, or both. If a student suffers an injury that the university could have reasonably foreseen, and if the university had established an adequate relationship with that student to justify imposing a duty of care to prevent that injury, it may be held liable for the student's injuries. Let us consider the two most common theories for finding a special relationship between colleges and their students.

1. The Landowner-Invitee Analogy

The first theory student plaintiffs use to establish a duty of care is based on a landowner-invitee relationship between colleges and students. This theory rests on the premise that the manager or owner of a place used by the public owes a duty to keep the premises reasonably safe for those whom for business reasons it invites on to its land. Consider a landowner who invites another individual to enter the property to assist in performing repairs. The landowner may be held liable for injuries the invitee sustains if 1) the landowner knew or should have known of the risk of harm, 2) the invitee had no actual knowledge of the potential harm, and 3) the landowner did not exercise reasonable care in preventing harm to the invitee. [52]

Courts have sometimes been willing to apply this theory to colleges, even, on occasion, to non-student invitees at campus events. An Indiana court found the University of Notre Dame liable for injuries sustained by a non-student

attendee at a football game.[53] The court found that Notre Dame was aware that alcoholic beverages are consumed on its premises before and during football games and that, while the university could not identify the particular danger posed by the inebriated individual who injured that specific visitor, it did have reason to know that some spectators will become intoxicated and pose a general threat to the safety of others. Therefore, said the court, Notre Dame had a duty to take reasonable precautions to protect from injury those who attend its football games.

Under the landowner-invitee theory, courts have also held universities liable for school-related accidents involving injuries in student dormitories and fraternity hazing incidents. In *Furek v. University of Delaware*,[54] the university promulgated and publicized a policy against fraternity hazing, yet hazing continued unabated on the Delaware campus for a period of at least five years before Furek's injuries. The state superior court found Delaware liable for injuries to a student harmed by hazing, holding that when a university has involved itself in the regulation of certain risky student practices, it could not abandon what the court termed its "residual duty of control" in taking on the identified harm.[55] Under the *Furek* reasoning, once a university purports to identify and address problems associated with risky behavior, it cannot shirk the responsibility it took on in doing so and may be held liable for injuries resulting from incidents that arise as a result of a risk management program's failures. The *Furek* court determined that Delaware had a duty of care to prevent the harm to the student because the fraternity was located on university property and the university was aware of the "dangerous propensities of the fraternities as they related to hazing."[56]

Under the landowner-invitee theory, courts have also held universities liable for school-related accidents involving injuries in student dormitories and fraternity hazing incidents.

In analyzing foreseeability, courts do not typically distinguish between lawful and unlawful activities, such as underage drinking or illicit drug use. On the contrary, if a university takes steps to acknowledge or identify a specific harm on its campus, even if the activity is prohibited both by law and by campus policy, some courts may apply *Furek*'s reasoning. This could lead a court to find that if a university is aware that drug overdoses have occurred on campus and has sought to regulate drug use, through such measures as promulgating university policies or campus risk management plans, those efforts, in themselves, may be viewed as tacit recognition of the potential for harm. This could be of particular concern for universities that have been the site of previous student overdoses, as those institutions are plainly on notice of the potential for serious opioid-related harm.

2. The "Special Relationship" Theory

The second theory student plaintiffs argue is that colleges owe a duty of care because of an intrinsic "special relationship" with their students. Such relationships can arise when a party assumes responsibility for another's safety or deprives another of his normal opportunities for self-protection.[57] The rationale behind this theory is that universities routinely regulate their students' daily activities and therefore take on the responsibility to ensure student safety, for instance by creating and enforcing campus policies. Some courts have found that such a "special relationship" between universities and their students grounds a duty of reasonable care. In *Kleinknecht v. Gettysburg College*, a student lacrosse player died of cardiac arrest during practice.[58] His parents filed a wrongful death and survival action against the college, and the district court found for all defendants. On appeal, however, the appellate court reversed, holding that the college's duty of care to the deceased student as an intercollegiate athlete did include a duty to provide prompt, meaning almost immediate, emergency medical service while he was engaged in school-sponsored athletic activity.[59] The appellate court also found that the college's failure to protect against such a risk was not reasonable and was thus a breach of the standard of care.[60]

Other cases have considered whether a student's residence in a university dorm is grounds to find a special relationship sufficient to impose a duty of care. In *Schieszler*

v. Ferrum College, the estate of a college student who committed suicide in his dormitory room sued the college for wrongful death.[61] The court noted that a special relationship can give rise to a duty to take affirmative action to assist or protect another. Considering all factors relevant to the relationship, including that the student plaintiff lived in an on-campus dormitory, had been required to attend anger management counseling, and was previously discovered injuring himself, the court imposed a duty on the college and found it liable for the student's death.[62]

From cases such as these, it seems reasonable to anticipate that a college student coming to harm from opioid intoxication, or his estate if he dies, could claim that his college should have taken steps to reduce the risk. That from among its hundreds or more often thousands of students the college would have no way to identify a specific potential victim need not preclude recovery. If the plaintiff can establish the prevalence of opioid use and misuse on campus, and the probability that in some fraction of cases harm will ensue, he may well satisfy the foreseeability requirements discussed above. What must be foreseeable is not the identity of the potential victim, nor the time or place at which he will come to harm, nor the precise circumstances leading to his injury or death, but only that from among the student body some member(s) will probably get hurt from using opioids. As we have seen, harm can arise whether opioids are used lawfully or otherwise. In those cases where the use is illicit, the college may find no defense, as we can see from the alcohol cases. That a claim is brought, of course, is a far cry from saying it will succeed. But in some cases, in some jurisdictions, such an outcome seems plausible.

By no means is liability a foregone conclusion in opioid intoxication cases. Some courts have been less willing to find that the relationship between universities and their students is such that the school is under a duty of care to prevent certain harms. In *Jain v. State*, for example, a student committed suicide in his University of Iowa dorm room.[63] The court found that no special relationship existed between the university and the student giving rise to an affirmative duty to prevent a suicide. *Jain* may be distinguishable, however, from an instance where a student injures himself through opioid overdose. To take affirmative steps to reduce the probability of harm to the suicide, the university involved in *Jain* would have had to recognize the probability that the specific student involved would try to kill himself—although the *Ferrum College* court was willing to do just that. In other situations involving harm to students, however, identifying a specific student at risk is not essential to preventing the injury or harm. Taking affirmative steps to reduce the probability of harm to students who may suffer from an opioid overdose, for instance, would require no such specific identification of the students at risk. It would only be necessary to identify situations or locales where such harm may take place, such as in university dorms or at university-sponsored events where drug use is known to occur. In some cases, then, a university may be found to have a special relationship, and thus a duty to ensure safety, even though it cannot specifically identify students at risk for drug use and overdose, whether intentional or unintentional.

At least one court has expressly held, in *Bash v. Clark University*, that universities bear no liability for drug use injuries sustained by students, even if the overdose event occurred on campus property, finding that no such special relationship exists between a university and its students to prevent harm from overdose.[64]

Whether courts are expansive or restrictive in considering the duties of colleges towards students, one must recognize that the law evolves. According to the Supreme Court of Florida, for example, given advances in technology and equipment, such as development of portable AEDs, a trial court committed reversible error in granting summary judgment against the plaintiff-parents of a 15 year-old student who arrested and suffered anoxic brain injury at a school soccer match at which school representatives failed to deploy the AED purchased for use in case of cardiac arrest.[65]

The standard of care, then, is not fixed. *Bash* was handed down nine years ago, for example, well before the current heightened focus on opioid intoxication developed, and before a safe and effective antidote became available, specifically FDA approved for use outside a health care setting.

Breach

Recall the elements of the tort of negligence: duty, breach, causation, damages. After establishing a *prima facie* case of duty, a student plaintiff must prove breach. This requires

establishing the standard of care: The degree of prudence and caution required of the defendant. Then, plaintiff must demonstrate that the defendant breached its duty of care by failing to meet that standard. To determine whether a party has breached the applicable standard of care, courts often weigh the gravity and probability of the harm associated with such non-action against the societal burdens that correspond with imposing such responsibilities. This calculus was first articulated in a famous opinion by judge Learned Hand, utilizing a cost-benefit analysis to conclude that the owner of a sunken barge had a duty to the cargo owner to keep its employee aboard the vessel and the failure to do so was a breach.[66] Under Hand's formulation, a party is under a duty to act if the product of the probability of harm from not acting ("P") and the magnitude of that harm ("L") outweighs the burden of acting to prevent that harm ("B"). An actor is under a duty to undertake a safety precaution, said Judge Hand, if B<PL.

Under this reasoning, if a university has a duty of care to a student and does not take action to prevent a reasonably foreseeable harm, the university will be found to have unreasonably breached its duty of care if the burden of preventing the harm is outweighed by the product of the severity of the harm and the probability the harmful event will occur. In *Kleinknecht v. Gettysburg College*, the court examined whether the foreseeable risk was unreasonable and determined that the benefit and reduced risk of harm of taking potentially life-saving protective action in providing immediate medical care to the student athlete outweighed the burden of imposing such responsibilities on the college.[67]

An actor is under a duty to undertake a safety precaution if B<PL.

As we have seen, some courts are willing to find a special relationship between universities and their students obliging the college to take reasonable steps to protect its students. Changing circumstances in both the university setting and in pharmaceutical innovation have created new factors that strongly affect the determination whether a college has breached a duty to students. Learned Hand's calculus for breach could be applied here.

First, the severity of the potential harm ("L") in overdose cases is potentially catastrophic. Student plaintiff injuries resulting from overdose can be serious and frequently result in death.[68] Studies have demonstrated that young adult users of opioids for non-medical purposes are at high risk of both fatal and non-fatal overdose.[69]

Second, in determining the probability of harm ("P"), a court would likely find that university officials are now on notice of the drug use and misuse issues on their campuses. National initiatives to identify the risk to college-aged students argue for a need for collegiate action in helping to prevent overdoses and their consequences.[70] Acknowledging the harm drug use and overdose presents to students, many colleges have created drug policies; with the prodding of the Department of Education and the example of schools such as SUNY many more will likely follow.

It remains to consider a college's burden ("B") in seeking to prevent overdose harms. Student plaintiffs can point to the willingness of peer institutions, in the face of near-universal budget constraints, to create programs aimed at reducing risk. They can argue that the incremental cost to an institution of higher learning to train resident assistants, campus security personnel, or students themselves in resuscitation techniques is minimal and will likely succeed. They can point to the newly eased availability, outside the healthcare system, of safe and effective opioid antidotes, such as the naloxone auto-injector, designed to be used by laypersons during a suspected opioid emergency.

The more drug use and overuse rates on college campuses continue to rise and the burden of preventing opioid overdose decreases, the more likely it is that a college could be found to have breached its duty to care for its students by failing to prevent the harm of overdose on its campus. By failing to acknowledge the increasing prevalence of overdoses on college campuses and failing to take steps to adequately prevent the associated harms, colleges needlessly risk exposing themselves to negligence claims.

Collegiate Reputation

Even if litigation never ensues after an overdosing student dies on campus, the university where that occurred faces significant risk of reputational damage. In this era

of the 24-hour news cycle, and the media's fascination with harm, coverage is apt to be both rapid and extensive. The impact upon current students, alumni support, and applications will likely be adverse. One need but consider the impact of the sexual abuse scandal at Penn State[71] or the murderous rampage at Virginia Tech[72] to appreciate the destructive power of adverse publicity.

Conclusion

In no reported case has the estate of a student dead from opioid intoxication sued a college, successfully or otherwise. The probability, however, is that at some point such a theory will be advanced. The defense, at some cost, may prevail, especially in jurisdictions hostile to the notion that a "special relationship" exists between institutions of higher learning and their students. In other jurisdictions, however, a plaintiff may be able to "get to the jury" and win a verdict. Even where litigation is not brought, news of a preventable, drug-related campus death could have substantial impact and not for the better. Colleges should evaluate the risks and act on the judgments they form.

The problem of opioid intoxication is unlikely to disappear soon and is profoundly troublesome for our entire society. Forward-thinking universities, however, could not only provide a measure of protection for their students but also distinguish themselves from their peers by taking steps to understand and cope with the problem. A number of colleges already have; multiple measures are available to improve matters. The law demands that each of us act as the "reasonable person" would. We may have reached a point today where failing to acknowledge and prepare for opioid intoxication on college campuses may fall short of what is reasonable, and hence required. At the very least, we should recognize that advocates are prepared to so claim.

About the Author

Joseph P. McMenamin is the AV-rated principal at McMenamin Law Offices, PLLC, in Richmond, Virginia. MLO is a health law boutique serving health care providers and life sciences companies, focusing on legal issues pertinent to distance care, general health law, risk management, and reimbursement. Dr. McMenamin has 30 years of experience in defending health care providers and pharmaceutical, medical device, and biotech companies against a variety of allegations in state and federal court. He has advised these clients on Internet and marketing communications, informed consent, risk management, regulatory, and contract issues. Dr. McMenamin has counseled hospitals, nursing homes, physicians, and other health care providers with respect to a wide array of legal issues as well, including their interactions with regulated industry.

Dr. McMenamin's consultancy, MDJD, LLC, addresses an array of medicolegal issues. Among them are matters as varied as hospital privileges, HIPAA and patient privacy, EMTALA, risk management, professional licensure, employment contracts, clinical trials, disaster preparedness, the Virginia Birth Injury Fund, pain management issues, and reimbursement. MDJD also provides a medical record review service for litigants in personal injury and wrongful death cases. In aid of such litigants, MDJD offers expert identification and development of alternative causation theories.

Dr. McMenamin is general counsel for the Virginia Telehealth Network and a member of the Center for Telemedicine and eHealth Law ("CTeL") Legal Resource Team. He is a member of the Board of Advisors of the *Medical Information Technology Law Report*, and serves on the advisory boards of CW Optics, Inc. and of the Regulatory Harmonization Institute. He is also an associate professor in the Department of Legal Medicine at Virginia Commonwealth University, Board-certified in Legal Medicine, and a Fellow of the College of Legal Medicine.

Before starting his own practice, Dr. McMenamin was a partner at McGuireWoods, LLP for 20 years. Previously, he practiced emergency medicine at hospitals in Pennsylvania and Georgia for seven years while engaging in specialty training and legal education. He is a former member of the boards of directors of the Medical Society of Virginia Insurance Agency and of the Richmond Ambulance Authority.

Dr. McMenamin has authored or co-authored numerous articles and chapters on a wide array of legal and other topics. He has also given hundreds of presentations at local, state, national, and international meetings of lawyers, doctors, risk managers, business continuity experts, regulatory professionals, and other groups on this area of expertise.

Endnotes

[1] The author wishes to acknowledge that he serves as a consultant to Kaleo Pharma, makers of Evzio, a brand of naloxone; and the author would like to thank Ashley Howe, J.D. for assistance with research.

[2] Sondra vanderVaart, et al., "CYP2D6 Polymorphisms and Codeine Analgesia in Postpartum Pain Management: A Pilot Study," *Therapeutic Drug Monitoring*, 33 no. 4 (2011) 425.

[3] Yan Xu and Ana Johnson, "Opioid Therapy Pharmacogenomics for Noncancer Pain: Efficacy, Adverse Events, and Costs," *Pain Research and Treatment* (2013) 1–8.

[4] Stephen M. Thielke, et al., "Age and Sex Trends in Long-term Opioid Use in Two Large American Health Systems Between 2000 and 2005," *Pain Medicine*, 11, no. 2 (2010) 248–256.

[5] President's Letter to Congress, Executive Office of the President, National Drug Control Strategy, 2011. https://www.whitehouse.gov/sites/default/files/ondcp/ndcs2011.pdf (hereinafter, "Control Strategy").

[6] CDC, WONDER [database], 2013. http://wonder.cdc.gov.

[7] Ibid.; Jeffrey A. Gudin, et al., "Risks, Management, and Monitoring of Combination Opioid, Benzodiazepines, and/or Alcohol Use," *Postgrad Medicine* 125, no. 4 (2013) 115–130.

[8] Center for Disease Control and Prevention, "CDC Grand Rounds: Prescription Drug Overdose – a U.S. Epidemic," *Morbidity and Mortality Weekly Report* 61, no. 1 (2012) 10–13.

[9] Center for Disease Control and Prevention, "QuickStats: Rates of Deaths from Drug Poisoning and Drug Poisoning Involving Opioid Analgesics — United States, 1999–2013," *Morbidity and Mortality Weekly Report* 64, no. 1 (2015) 32.

[10] SAMHSA Center for Behavioral Health Statistics and Quality. Drug Abuse Warning Network, 2011: National Estimate of Drug Related Emergency Department Visits, 2011 (Between 2004 and 2011, prescription opioid emergency department visits almost tripled, from approximately 173,000 to 488,000).

[11] Evan Edwards, et al., "Comparative Usability Study of a Novel Auto-Injector and an Intranasal System for Naloxone Delivery," *Journal of Pain and Therapy*, DOI 10.1007/s40122-015-0035-9 (2015).

[12] DHHS, [Assistant Secretary for Planning and Evaluation] Issues Brief, "Opioid Abuse in the U.S. and HHS Actions to Address Opioid-Drug Related Overdoses and Deaths," March 26, 2015, 1, http://aspe.hhs.gov/sp/reports/2015/OpioidInitiative/ib_OpioidInitiative.cfm (hereinafter ASPE).

[13] Michael A. Yokell, et al., "Presentation of Prescription and Nonprescription Opioid Overdoses to US Emergency Departments," *Journal of the American Medical Association Internal Medicine* (online Oct. 27, 2014).

[14] Kohei Hasegawa, et al., "Epidemiology of Emergency Department Visits for Opioid Overdose: A Population-Based Study," *Mayo Clinic Procedures* 89, vol. 4 (2014) 462-471.

[15] Control Strategy, 2, https://www.whitehouse.gov/sites/default/files/ondcp/ndcs2011.pdf.

[16] National Council on Patient Information and Education, "'Get the Facts' Prescription Drug Abuse on College Campuses," http://www.talkaboutrx.org/documents/GetTheFacts.pdf.

[17] SAMHSA, Center for Behavioral Health Statistics and Quality, "Results from the 2013 National Survey on Drug Use and Health: Summary of National Findings," NSDUH [National Survey on Drug Use and Health] Series H-48, HHS Publication No. (SMA) 14-4863, 2014, 27. http://www.samhsa.gov/data/sites/default/files/NSDUHresultsPDFWHTML2013/Web/NSDUHresults2013.pdf (hereinafter, "2013 Survey").

[18] National Council on Patient Information and Education, "'Get the Facts' Prescription Drug Abuse on College Campuses," http://www.talkaboutrx.org/documents/GetTheFacts.pdf, citing NSDUH (2008) and Arria (2008).

[19] 2013 Survey.

[20] David Frank, et al., "High Risk and Little Knowledge: Overdose Experiences and Knowledge among Young Adult Nonmedical Prescription Opioid Users," *International Journal of Drug Policy* 26, vol. 1 (2015) 84–91.

[21] FDA Blueprint for Prescriber Education for Extended-Release and Long-Acting Opioid Analgesics 12/2014. http://www.fda.gov/downloads/Drugs/DrugSafety/InformationbyDrugClass/UCM277916.pdf. 22

[22] M. Boom, et al., "Non-analgesic Effects of Opioids: Opioid-Induced Respiratory Depression," *Current Pharmaceutical Design* 18, vol. 37 (2012) 5994–6004.

[23] Mt. Sinai Hospital, "Anoxic Brain Damage," 2015, http://www.mountsinai.org/patient-care/health-library/diseases-and-conditions/anoxic-brain-damage (anoxic brain damage in as little as 4 minutes).

[24] Edward W. Boyer, "Management of Opioid Analgesic Overdose," *New England Journal of Medicine* 367, vol. 2 (2012) 146–155.

[25] See, e.g., Angela Clark, et al., "A Systematic Review of Community Opioid Overdose Prevention and Naloxone Distribution Programs," *Journal of Addiction Medicine* 8, vol. 3 (2014) 53-63.

[26] "About Project Lazarus," http://www.projectlazarus.org/about-project-lazarus.

[27] Michael Botticelli, "Prescription Drug Abuse: The National Perspective," June 11, 2014, http://www1.villanova.edu/content/villanova/studentlife/prescription/materials/_jcr_content/pagecontent/download_1/file.res/Botticelli percent20Presentation percent20Slides.pdf.

[28] William Matthews, Harm Reduction Coalition, "Community Based Opioid Overdose Prevention: The Role of Naloxone," http://www.drugpolicy.org/docUploads/Matthews_OD_Prev_Fr_9a.pdf.

[29] Control Strategy, 28.

[30] D.C. Seo, et al., "The Effect of a Smoke-free Campus Policy on College Students' Smoking Behaviors and Attitudes," *Preventive Medicine* 53, vols. 4–5 (2011) 347–352.

[31] SUNY, "Heroin Abuse Prevention," http://system.suny.edu/university-life/alcohol-and-other-drug-prevention/heroin/.

[32] Daniel Helfand, "Candlelight Vigil Aims to Raise Awareness and Remember Those Lost to Prescription Drug Abuse (2013)," http://pharmacy.osu.edu/news/candlelight-vigil-aims-raise-awareness-and-remember-those-lost-prescription-drug-abuse.

[33] WBNS, "Preventing Drug Abuse," http://www.10tv.com/content/sections/video/index.html?ooid=xhbDNoaDqgaog0S3ogA9nb2t6YUaBm21&cmpid=share.

[34] Emily Keeler, "Ohio State to Hold Collegiate Prescription Drug Abuse Prevention and Recovery Training," 2013, http://pharmacy.osu.edu/news/ohio-state-hold-collegiate-prescription-drug-abuse-prevention-and-recovery-training.

[35] ROSEMANUNIV, "USN Student Group Joins Effort To Combat Drug Misuse and Abuse," 2010, https://univsonev.wordpress.com/2010/01/19/usn-student-group-joins-effort-to-combat-drug-misuse-and-abuse/.

[36] Brian Overholser and David Foster, "Opioid Pharmacokinetic Drug-Drug Interactions." *American Journal of Managed Care* 17 Suppl. 11 (2011) S276-87.

[37] Theodore Stanley, "Anesthesia for the 21st Century," *Baylor University Medical Center Proceedings* 13, vol. 1 (2000) 7–10, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1312206/.

[38] MedLine Plus, "Opioid Intoxication," April 2013, http://www.nlm.nih.gov/medlineplus/ency/article/000948.htm.

[39] J. Strang, et al., "Overdose Training and Take-Home Naloxone for Opiate Users: Prospective Cohort Study of Impact on Knowledge and Attitudes and Subsequent Management of Overdoses," *Addiction* 103, vol. 10 (2008) 1648-57.

[40] Substance Abuse and Mental Health Services Administration. *SAMHSA Opioid Overdose Prevention Toolkit*. HHS Publication No. (SMA) 14-4742. Rockville, MD: Substance Abuse and Mental Health Services Administration, 2014, http://store.samhsa.gov/product/Opioid-Overdose-Prevention-Toolkit-Updated-2014/SMA14-4742 .

[41] Caleb Banta-Green, et al., "Police Officers' and Paramedics' Experiences with Overdose and their Knowledge and Opinions of Washington State's Drug Overdose-Naloxone-Good Samaritan Law," *New York Academy of Medicine Journal of Urban Health* 90, vol. 6 (2013) 1102.

[42] Douglas C. Throckmorton, "Opioid Auto-Injector Can Help Prevent Overdose Deaths," *FDA Voice*, April 3, 2014, http://blogs.fda.gov/fdavoice/index.php/2014/04/opioid-auto-injector-can-help-prevent-overdose-deaths/.

[43] WHO, "Information Sheet on Opioid Overdose," November 2014, http://www.who.int/substance_abuse/information-sheet/en/.

[44] Naloxone hydrochloride [prescribing information] South El Monte, CA; International Medication System, Limited, 2011. If opioids are taken in combination with other sedatives or stimulants, however, naloxone may be helpful.

[45] Medscape "FDA Okays Handheld Autoinjector for Opioid Overdose," April 3, 2014, http://www.medscape.com/viewarticle/823039.

[46] It is estimated that the average EMS response time is 9.4 minutes. National EMS Information System (NEMSIS), http://www.nedarc.org/emsDataSystems/nemsisReports/2010_11EMSTimes.html.

[47] CDC Grand Rounds: "Prescription Drug Overdoses — a U.S. Epidemic," *Morbidity and Mortality Weekly Report* 61, vol. 1 (January 13, 2012) 10–13, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6101a3.htm.

[48] ASPE, 6–8.

[49] *Control Strategy*, 16–17.

[50] ASPE, 4.

[51] Andrew Rhim, "The Special Relationship Between Student-Athletes and Colleges: An Analysis of a Heightened Duty of Care for the Injuries of Student-Athletes", *Marquette Sports Law Journal* 7, issue 1 (1996) 329, 332, http://scholarship.law.marquette.edu/sportslaw/vol7/iss1/9.

[52] *Burrell v. Meads*, 569 N.E.2d 637 (Ind.1991).

[53] *Bearman v. Univ. of Notre Dame*, 453 N.E.2d 1196 (Ind. Ct. App. 1983).

[54] *Furek v. Univ. of Delaware*, 594 A.2d 506 (Del. 1991).

[55] Ibid., 520.

[56] Ibid., 515.

[57] *Beach v. Univ. of Utah*, 726 P.2d 413, 414–15 (1986), citing Restatement (2d) of Torts § 314(A) (1964).

[58] *Kleinknecht v. Gettysburg College*, 989 F.2d 1360 (1993).

[59] Ibid., 1370. "Though the specific risk that a person like Drew would suffer a cardiac arrest may be unforeseeable, the Kleinknechts produced ample evidence that a life-threatening injury occurring during participation in an athletic event like lacrosse was reasonably foreseeable."

[60] Ibid., 1360.

[61] *Schieszler v. Ferrum College*, 236 F.Supp.2d 602 (W.D. Va. 2002).

[62] Ibid., 609–610.

[63] *Jain v. State,* 617 N.W.2d 293 (Iowa 2000).

[64] *Bash v. Clark University*, 22 Mass.L.Rptr. 84 (2006).

[65] *Limones v. School Board of Lee County*, No. SC13-932 (Fla. 2015).

[66] *United States v. Carroll Towing Co.*, 159 F.2d 169 (1947).

[67] *Kleinknecht v. Gettysburg College*, 989 F.2d 1360, 1370 (1993).

[68] Boom, 5994–6004.

[69] Frank, 84–91.

[70] Control Strategy, 16–17. Searching for "university drug policy" on Google yields thousands of relevant results for drug policies instituted on campuses across the United States. See, https://www.google.com/?gws_rd=ssl#q="university+drug+policy"+.

[71] See, e.g., J. Luciew, "Three Years after Jerry Sandusky Scandal, Fallout for Penn State, NCAA is Hotter than Ever," http://www.pennlive.com/midstate/index.ssf/2014/11/three_years_after_jerry_sandus.html.

[72] Z.C. Sampson, "5 Years After The Virginia Tech Massacre, Colleges Gauge Threats," *Huffington Post College* (2012), http://www.huffingtonpost.com/2012/04/14/5-years-after-the-virgini_n_1425749.html.

Climate is what we expect. Weather is what we get.

—Mark Twain (1835-1910),

American Author and Humorist

Boom! Lightning Liability at University Athletic Events

| *Jon Cross, Marshall Dennehey Warner Coleman & Goggin*

Introduction

The occasional thunderstorm is rarely seen as a personal danger at sporting events. Lightning, however, is the second leading cause of weather-related deaths, taking an average of 70 lives per year and injuring 2.5 times as many.[1] While the chances of being struck by lightning are roughly 1 in 500,000[2], it is important to understand that the odds increase significantly when a thunderstorm is in the area and safety precautions have failed to be met.

The higher education risk management community needs to recognize that lightning strikes during athletic activities may result in personal injury lawsuits against the university as well as its administrators, coaches, and referees.[3] At those universities where sporting events are televised, broadcast companies may also be held liable if the decision to play the game for the sake of money and TV exposure gets in the way of safety. Colleges have responsibility for the safety of student athletes and the spectators at a sporting event. A failure to have preventative measures in place and a failure to follow such measures and safety precautions may lead to an injury associated with lightning and lawsuits against the university.

Lightning is the second leading cause of weather-related deaths, taking an average of 70 lives per year and injuring 2.5 times as many.

College Football Lightning Cancellation

It is rare for college football games to be delayed or cancelled due to weather conditions, but it does happen. On August 30, 2014, fans gathered at the University of Florida expecting to see a 7:00 p.m. football game against Idaho.[4] However, mother nature had a different idea. Half an hour before kickoff, a lightning strike turned the skyline into a dangerous laser show. Fans, players, and staff scrambled for cover. Then it got worse. Massive storms moved in pushing the start of the game to 9:48 p.m. During the delay, teams retreated to the locker rooms and fans were properly encouraged to go next door to the O'Connell Center to escape the danger.[5]

The Southeastern Conference has a policy that requires at least a 44-minute delay if lightning is detected within eight miles of the stadium.[6] This 44-minute period allows for a 30-minute break clear of local lightning strikes, a 10-minute warm-up for the players, and a 4-minute television pre-game show. At the Florida game, each subsequent lightning bolt resulted in the kick-off being delayed another 44 minutes. The extreme weather delayed the start of the game by 2 hours and 48 minutes.

Once the game finally started, Florida's Valdez Showers (irony noted) returned the opening kickoff for 64 yards. More lightning was then detected close to the stadium. Again, the teams and fans retreated to safety. At 10:40 p.m. the game was officially called off for unsafe field conditions.

Metal Bleachers Are Prime Targets

According to the National Weather Service, in 2014 there were 26 lightning fatalities in the United States. Six deaths occurred in Florida, three in Wisconsin, two each in Arizona, Arkansas, Colorado, Georgia, and Massachusetts, and one in Pennsylvania, among a few other states.[7] While deaths from lightning strikes in the U.S. are low compared with other natural disasters, 45 percent of such deaths occur in open areas such as sports fields, making stadiums with metal bleachers prime targets.[8]

Duty to Warn, Supervise, and Detect

Those who get struck by lightning or family members of an individual who dies due to a lightning strike may seek to file a lawsuit to assign blame and recover damages. College coaches, administrators, and referees have a duty to protect the student athletes and spectators. The duty is to act reasonably under the circumstances while understanding that not every act can prevent all unfortunate events and acts of God.

Claims for negligence may allege serious injuries from a lightning strike due to the college's failure to (1) adequately inform of the hazards of lightning; (2) detect lightning in the area; (3) use available lightning detection equipment; (4) warn of the presence of lightning; (5) have an effective evacuation plan; (6) instruct and supervise the evacuation; (7) provide a safe shelter at convenient locations; (8) provide proper post-injury treatment.

Lightning Lawsuits and Settlements

There have been a number of lightning-related lawsuits inherent to athletic events that are played outside on open fields. In New Jersey a lawsuit was brought by a golfer who was struck by lightning on a golf course.[9] In response to the lawsuit, the Superior Court opined that a golf club owes a duty of reasonable care to implement its safety precautions properly. The court did not go so far as to hold that clubs have an absolute duty to protect their patrons from lightning strikes, as it recognized the defense that sometimes a lightning strike can be an act of God. However, the court made clear that clubs have a duty to post signage that details what, if any, safety procedures are being utilized to protect its patrons from lightning. If a particular club uses no safety precautions, its signage must inform golfers that they "play at their own risk" and that no safety procedures are being utilized to protect golfers from lightning strikes.

Claims for negligence may allege serious injuries from a lightning strike due to a college's failure to inform, detect, warn, evacuate, and provide shelter and medical care.

The New Jersey court further recognized that existing technologies are available to detect and warn of lightning. It refrained from finding that the use of the latest technology is required because this greater duty may be cost prohibitive. The court did find, however, that if a club chooses to utilize a particular safety feature, it owes a duty of reasonable care to its patrons to utilize it correctly. This latter standard means, for example, that if a club builds shelters, it must build lightning-proof shelters; if the club has an evacuation plan, the plan must be reasonable and must be publicly posted; if a club uses a siren or horn system, the golfers must be able to hear it and must know what the signals mean; and if the club uses a weather forecasting system, it must use one that is reasonable under the circumstances.

In a separate New Jersey lawsuit, a school board was sued after a high school baseball player was struck by lightning while playing center field.[10] The player remained in a vegetative state. A lawsuit was brought against the school district and umpire alleging they had breached their duty to supervise and control the game, which included making decisions regarding the postponement or termination of the game due to imminent electrical storms. The New Jersey Board of Education settled the claim for $2.6 million.[11]

In Texas on August 26, 2014, a youth soccer player was struck by lightning in the stomach during soccer practice.[12] He suffered brain damage and cannot speak, hear or move his legs. A lawsuit was filed alleging that the league did not follow proper weather procedures, including failing to appoint a weather monitor, failing to supply or use a lightning detection system, and failing to get the players off the field. The pending lawsuit seeks $10 million in damages.[13]

Duty to Provide a Safe Shelter

In addition to detecting liability and stopping the game, proper risk management includes having a plan to evacuate and enforce the plan. Many times, games and practices are stopped, but the players simply stand around waiting out the storm. There is a duty to get both the players and spectators to a safe area.

For example on August 6, 2013, the Georgia Southern University football team moved practice up an hour to avoid incoming bad weather, but practice was properly stopped when lightning was detected in the area.[14] Georgia Southern does not have an indoor practice facility, so the team moved toward a nearby pavilion to wait out the storm. However, one player standing near the edge of the structure was injured when lightning struck a nearby tree. He was taken to a local medical center where he was evaluated and, fortunately, released to campus later that day – a very close call.

Duty to Administer Medical Care

In the event that a person is struck by lightning, a coach or athletic trainer should not hesitate to assist them. A failure to properly administer medical care could result in added liability. Unlike victims of electrical incidents, a lightning strike does not carry a charge so the individual may be safely handled.[15] Colleges should ensure that coaches, athletic trainers, doctors, and additional pertinent staff are professionally trained in life-saving first aid measures and can properly perform mouth-to-mouth resuscitation, CPR, and administer an automated external defibrillator (AED).[16]

Lightning Personal Injury Claims

People who get struck by lightning primarily suffer an injury to the nervous system, often with brain injury and nerve injury.[17] Serious burns can also occur.

There are a variety of personal injury claims which may arise due to a lightning strike. Individuals who do not suffer cardiac arrest at the time of the incident may experience lesser symptoms such as muscle soreness, headache, nausea, stomach upset, and other post-concussion types of symptoms including mild confusion, memory slowness or mental clouding, dizziness, and balance problems. However, many victims face longer-term problems which may include issues coding new information and accessing old information, problems multi-tasking, personality changes, inattentiveness or forgetfulness, headaches, chronic pain from nerve injury, ringing in the ears, dizziness or balance problems, and irregularities in sleep patterns.[18]

People who get struck by lightning primarily suffer an injury to the nervous system, often with brain injury.

Lightning Risk Management Policy

To reduce the liabilities associated with lightning strikes, colleges should have a written athletic department lightning policy. Elements of such a plan may include the following:

1. Signage

Provide warnings about thunder and lightning and explain the devices being used on campus. Also, promote National Weather Service lightning safety slogans such as "No Place Outside is Safe When Thunderstorms are in the Area" or "Half an Hour Since Thunder Roars, Now it's Safe to Go Outdoors."

2. Establish a Chain of Command

Identify the person who makes the decision to suspend a practice, pre-game activities, or a game. Also, the policy should establish who is to disseminate lightning information.

3. Weather Watcher

Designate a "weather watcher" who will monitor the National Weather Service about the local weather and may consult with available meteorologists. Also, consider who will be responsible for any detection system utilized on campus and to report the information.

4. Suspension of Activity

The average distance from one lightning strike to the next is approximately 2 to 3 miles yet can be as much as 10 miles. Therefore, while a storm may be several miles from your location, the very next strike could be on top of you. If lightning strikes within 10 miles of a stadium, recent National Collegiate Athletic Association policy requires a public announcement advising fans to evacuate. Based on recent NCAA guidelines, if lightning hits within 6 miles, players and officials are required to leave the field, and the game is delayed. The game must be delayed 30 minutes after the last strike of lightning has been detected within that 6-mile radius.[19]

5. Safe Shelter

Identify safe locations from lightning hazards in advance of events such as any building normally used by people, for example an enclosed and grounded building with plumbing and electrical wiring. In absence of a sturdy, frequently inhabited building, any vehicle with a hard metal roof (not a convertible or golf cart) and rolled up windows will provide a safe shelter. Know how long it will take to evacuate the premises and get people to the safe venues. Direct spectators to the nearest safe place and ensure a safe and orderly evacuation.

6. Unsafe Areas

Know what areas players and spectators should avoid such as metal bleachers, metal fences, open areas, water/swimming pools, tall trees, towers, golf carts, and mowers, and avoid being the tallest object in the area.

7. Emergency Medical Plan

Have a plan for rescuers and emergency personnel who are properly trained in mouth-to-mouth resuscitation, CPR, use of the AED, first aid, and other emergency measures.

8. Education

Review the lightning policy annually with all administrators, coaches, and game personnel. Also, review the policy with student athletes at the start of the season. Ensure there is an awareness of the dangers of lightning and that coaches and staff are committed to following the guidelines.

Lightning Detection Technology

Before recent technology became available, the traditional tech-free way of assessing lightning risk was the 30/30 rule or the flash-to-bang rule.[20] This was the easiest and most convenient method to determine the distance from the last lightning strike, but this method cannot predict where the next strike will occur. Begin a count that is equivalent to one second at the time you see a flash of lightning, and continue counting until you hear the thunder. Divide that number by 5 to determine the distance in miles that the strike was from you. For example, if you count 30 seconds between lightning and thunder, this indicates the strike was approximately 6 miles away. However, a reasonable coach or administrator should not be counting when they see lightning; rather, they should get the athletes off of the field and spectators out of the stadium. Quite frankly, if it is heard or seen, it is close enough to pose a threat.

University risk managers may want to consider new technology that is available in the form of lightning detection equipment and lightning prediction equipment.[21] The former tracks actual lightning strikes within a set parameter around a facility, and the latter identifies electrostatic energy conditions conducive to lightning activity. With the lightning prediction system, a horn sounds and flashing lights are emitted when lightning is detected within a 10-mile radius, and live electronic alerts are sent to designated cell phones and email addresses. In considering such technology, colleges should seek professional advice regarding purchasing the desired equipment. Also, for individuals there now exist many cell phone applications that can identify the distance of lightning.

The use of technology can help take the guesswork out of when to cancel or postpone a practice or game and keep individuals safe. Coaches, referees, game officials, and TV stations do not like to postpone or cancel games. For that reason, the use of a lightning system will remove the human decision-making factor, which in turn may save a life and reduce the potential of liability.

Before recent technology became available, the traditional tech-free way of assessing lightning risk was the 30/30 rule or the flash-to-bang rule.

Common Sense Must Prevail

Even if the college invests in providing the utmost care, such as purchasing a lightning detection and prediction equipment system, common sense must still prevail. The warning signs from the technology must be taken seriously. The coaches and game officials must stop the contest and make sure the players and spectators do in fact seek proper indoor shelter.

Risk managers should be aware that if an injury does occur on campus and the college is blamed, economic and business factors may warrant consideration of a settlement either before a lawsuit is filed or during the litigation process. The cost of litigation could be significant and the amount of damages could be substantial if the injured party has suffered some of the most severe lightning strike symptoms. However, if the college believes it was not negligent because appropriate risk management policies and procedures were followed, settlement may not be in its best interest as it may encourage other types of lawsuits for claims relating to a failure to supervise, warn, instruct, or protect.

The unpredictability of lightning presents significant

challenges for university risk management professionals. Athletic departments must be proactive in planning and follow procedures to reduce danger to individuals and associated liabilities due to lightning. In this ball game, it's not three strikes, but just one lightning strike, and you must get out!

About the Author

Jon Cross is an attorney at Marshall Dennehey Warner Coleman & Goggin and a former camp owner, Division I college baseball coach, and high school baseball coach. He is a member of the law firm's amusement, sports, and recreation department and practices law in the Philadelphia, Pennsylvania, office. The law firm has offices in New York, New Jersey, Pennsylvania, Ohio, Delaware, and Florida. He may be reached at jecross@mdwcg.com.

Endnotes

1 National Weather Service. "NWS Lightning Safety," http://www.lightningsafety.noaa.gov.

2 Wikipedia, "Lightning Strike," http://en.wikipedia.org/wiki/Lightning_strike.

3 By way of comparison, see: NBC Sports, "Widow of fan killed by lightning sues Pocono Raceway and NASCAR," last modified August 6, 2014, http://motorsportstalk.nbcsports.com/2014/08/06/widow-of-fan-killed-by-lightning-sues-pocono-raceway-nascar/.

4 ESPN, "Idaho-Florida game suspended due to unsafe field conditions," last modified August 30, 2014, http://scores.espn.go.com/ncf/recap?gameId=400548399.

5 *Florida Times-Union*, "Lightning postpones Gators' season opener forcing fans to head for cover Lightning postpones Gators' season opener forcing fans to head for cover," last modified August 30, 2014, http://jacksonville.com/sports/college/florida-gators/2014-08-30/story/lightning-delays-gators-season-opener-forcing-fans.

6 Id.

7 National Weather Service, "National Lightning Fatalities," www.lightningsafety.noaa.gov/fatalities/fatalities14.shtml.

8 *Bloomberg Business*, "The Odds That Lightning Will Ruin Your Football Saturday," last modified September 3, 2014, http://www.bloomberg.com/bw/articles/2014-09-03/the-odds-that-lightning-will-delay-a-college-football-game.

9 *Maussner v. AC Country Club, Inc., et al*, 691 A. 2d (NJ Super. 1997).

10 *Krishan Thomas v. East Orange Board of Education et al.*, 2:2012cv01446 (NJ Dist. Ct., 2014).

11 Amateur Baseball Umpires' Association. "Lightning Strikes - Essex County Judge James S. Rothschild, Jr. has approved a $2.6 million settlement in a trust for Krishan Thomas," last modified August 2004, http://www.umpire.org/abua/august2004.pdf.

12 *Statesman*. "Family of boy struck by lightning sues," last modified September 9, 2014, www.statesman.com/news/news/local/family-of-boy-struck-by-lightning-sues/nhJkn/

13 Id.

14 Yahoo! Sports, "Georgia Southern player taken to hospital after lightning strike at practice," last modified August 21, 2013, http://sports.yahoo.com/blogs/ncaaf-dr-saturday/georgia-southern-player-taken-hospital-lightning-strike-practice-020027453.html.

15 National Oceanic & Atmospheric Administration, "Lightning Myths and Facts," www.lightningsafety.noaa.gov/myths.shtml.

16 Id.

17 National Oceanic & Atmospheric Administration, "Medical Aspects of Lightning," www.lightningsafety.noaa.gov/medical.shtml.

18 Id.; see also: Medscape, "Lightning Injuries," last modified September 26, 2014, http://emedicine.medscape.com/article/770642-overview.

19 NCAA Sport Science Institute, "Lightning Safety," http://www.ncaa.org/health-and-safety/lightning-safety.

20 *LiveScience*, "How Far Away is Lightning?" last modified June 25, 2013, http://www.livescience.com/37734-how-far-away-is-lightning-distance.html.

21 National Lightning Safety Institute, "Overview of Lightning Detection Equipment, Section 5.5.3," http://www.lightningsafety.com/nlsi_lhm/detectors.html.

We are healthy only to the extent that our ideas are humane.

—Kurt Vonnegut (1922-2007),

American Author

Minimize Potential Liabilities in Collegiate Sports Medicine Departments

| *Timothy Neal, ATC, Eric Quandt, JD, James Thornton, ATC, Jeffrey Anderson, MD*

Introduction

When collegiate sports medicine staff, other athletics department staff, and institutions fail to properly address student athlete safety and welfare issues, you can bank on facing potential liability.

But you can take steps to help enhance the safety and well-being of your student athletes while also limiting your institution's liability risk by reviewing the key areas that pose the most liability and by raising awareness among your institution's and athletic department's administrators, risk managers, and general counsel.

Manage Concussion Incidents

Start by reviewing the "Sports-Related Concussion" guideline in the 2013-2014 *National Collegiate Athletic Association Sports Medicine Handbook* (www.ncaapublications.com/p-4328-2013-14-ncaa-sports-medicine-handbook.aspx). That guideline thoroughly addresses a variety of important concussion-related topics. Ensure you also carefully examine the section "Concussion Diagnosis and Management" for critical guidance on diagnosis, concussion management, supervised graded program of exertion before medical clearance, and return to play. And be sure to adhere to the admonition included in that guidance: "Final clearance for a return to play should be provided by a physician or a physician's designee."

Also pay particular attention to the NCAA's health and safety materials on the NCAA website (www.ncaa.org/health-and-safety). The new guidelines, which aim to improve student athlete safety, are based upon an interassociation consensus. In addition to the guidelines for football practice contact, also consider the following two areas covered on the website:

Independent Medical Care for College Student Athletes

(1) An institutional medical line of authority should be established independently of a coach and in the sole interest of student athlete health and welfare. (2) Institutions should, at a minimum, designate a licensed physician (M.D. or D.O.) to serve as medical director, and that medical director should oversee the medical tasks of all primary athletics health care providers. (3) The medical director and primary athletics health care providers should be empowered with unchallengeable autonomous authority to determine medical management and return-to-play decision of student athletes.

Diagnosis and Management of Sport-related Concussion

(1) Institutions should make their concussion management plan publicly available, either through printed material, their website, or both. (2) A student athlete diagnosed with sport-related concussion shouldn't be allowed to return in the current game or practice and should be withheld from athletic activity for the remainder of the day. (3) The return to academics should be managed in a gradual program that fits the needs of the individual within the context of a multidisciplinary team that includes physicians, athletic trainers, coaches, psychologists/counselors, neuropsychologists, and administrators as well as representatives from academic areas (e.g., professors, deans, academic advisors) and disability services.

Develop a Concussion Plan

You should need to know when you should first remove a student athlete from practice or competition. The "NCAA Concussion Policy and Legislation" section in the 2013-2014 *NCAA Sports Medicine Handbook* provides information about the policy adopted in 2010 by the NCAA Executive Committee for institutions in all three divisions:

Institutions shall have a concussion management plan on file such that a student athlete who exhibits signs, symptoms, or behaviors consistent with a concussion shall be removed from practice or competition and evaluated by an athletics health care provider with experience in the evaluation and management of concussions. Student athletes diagnosed with a concussion shall not return to activity for the remainder of that day. Medical clearance shall be determined by the team

physician or his designee according to the concussion management plan.

Although it was not finally approved at the time of this publication, the NCAA reached a proposed settlement in its concussion lawsuit stating that: "under the proposed settlement agreement, all current and former NCAA student athletes in all sports and divisions who competed at an NCAA member school may qualify for physical examination, neurological measurements, and neurocognitive assessments.

The $70 million NCAA fund will go toward concussion testing and diagnosis—not as payment of damages. But the student athletes can sue individually for damages. The NCAA settlement doesn't prevent individual lawsuits by student athletes regarding mismanaged concussion assessment and care.

Address Use of Energy Drinks

Energy drinks contain high levels of caffeine and can lead to tachycardia, hypertension, obesity, and other medical problems, according to the American Academy of Pediatrics. Energy drinks become even more dangerous when mixed with alcohol, the AAP reported.

Nearly 40 percent of college students consumed energy drinks in the past month, according to an AAP survey of almost 800 college students. And consuming high levels of caffeine can place student athletes at risk of NCAA violations. In fact, student athletes are in violation when their caffeine levels, as measured in their urine, reveal that they drank the equivalent of about five to eight cups of coffee in one hour—or as few as one to three energy drinks.

"Energy drinks contain high, unregulated amounts of caffeine that may lead to significant morbidity in adolescents (cardiovascular effects, withdrawal symptoms, mixing with alcohol, association with substance abuse)," the AAP stated.

Clearly, energy drinks should be a subject of concern in developing an overall plan for the health, safety, and well-being of your student athletes.

Beware OTC Supplements

The cardiac risks of tachycardia and hypertension noted by the AAP are similar to the risk posed by over-the-counter dietary supplements containing ephedrine alkaloids banned by the U.S. Food and Drug Administration in 20014. In 2006 the U.S. Court of Appeals for the 10th Circuit in Denver upheld the FDA ban in a carefully reasoned decision (*Neutraceutical Corp. v. Von Eschenbach*, 459 F.3d 1033).

A surge in the use of supplements containing ephedrine alkaloids led to many reports of student athletes suffering severe side effects, including at least 10 Northwestern University football players, according to the American College of Sports Medicine.

The ACSM recommended that coaches, athletic trainers, parents, and health care professionals encourage optimal hydration and education student athletes about the disadvantages of using energy drinks. In fact, drinks like Red Bull, Lizard Fuel, and Adrenaline Rush all contain high doses of caffeine and might not even contribute to increased performance, the ACSM stressed.

Health concerns surrounding energy drinks have also been the subject of recent legislative activities. In 2013 in a press conference and a joint letter to the NCAA and the National Federation of State High School Associations, Illinois Senator Dick Durbin and his colleagues addressed concerns about the marketing of energy drinks at high school and collegiate athletic events. Alderman Edward M. Burke also last year chaired hearings before the Chicago City Council Health and Environmental Protection Committee focusing on the dangers of energy drinks.

Ensure that your concussion guidelines, recommendations, and policies are clearly understood by all of your institution's athletics care providers.

Raise Awareness of Plans

Ensure that your concussion guidelines, recommendations, and policies are clearly understood by all of your institution's athletics health care providers (athletic trainers and team physicians), coaches, athletics directors, risk managers, insurers, and all relevant institutional administrators—and implemented in a clearly-written concussion

management plan easily and publicly accessible in writing, through your website or both.

When you develop a concussion protocol for your athletics department, be sure to collaborate with experts knowledgeable about the sports medicine issues involved as well as all of the potential risks and liabilities.

Enhancing the health and safety of your student athletes in the context of protecting the legitimate interest of your institution and staff members should remain your ultimate goal.

About the Authors

Dr. Jeffrey Anderson graduated from the University of Michigan Medical School in 1990. Prior to University of Michigan, he earned his Bachelor of Arts in chemistry from North Park University in Chicago.

Dr. Anderson is currently the director of student health at University of Connecticut where he also served as the head team physician and director of sports medicine from 1994 to 2014. In addition to his work for the university, he also serves as an independent program administrator for the Major League Baseball and Major League Baseball Players Association Joint Drug Prevention and Treatment Program.

Timothy Neal is the former assistant director of athletics for sports medicine at Syracuse University, where he provides leadership and supervision of seven full-time athletic trainers and 10 graduate assistant athletic trainers. He's also a member of the New York State Board of Athletic Training and received the National Athletic Trainers' Association's Most Distinguished Athletic Trainer Award in 2010. Mr. Neal also received the 2013 New York State Athletic Trainers' Association Thomas Sheehan Award for his achievements in the athletic training profession in New York State.

Mr. Neal authored the "Catastrophic Incident in Athletics" guideline, and authored revisions in the "Mental Health: Interventions for Intercollegiate Athletics" guideline in the NCAA Sports Medicine Handbook. He served on the panel for the NCAA Concussion in Sport Medical Management Summit. He served as NATA Liaison to the NCAA Football Rules Committee from 2004-2009, writing language for the helmet contact penalty, defenseless opponent penalty, and the Horse Collar Tackle penalty in college football. He also wrote passages in the "Points of Emphasis" section of the NCAA Football Rules Book on concussions, hydration, and MRSA. In 2013 Tim served on the NCAA Student Athlete Mental Health Task Force.

Mr. Neal chaired the 2013 NATA "Recommendations in Developing a Plan to Recognize and Refer Student-Athletes with Psychological Concerns at the Collegiate Level Consensus" Statement, and again is serving as chair of the NATA consensus statement, "Recommendations in Developing a Plan to Recognize and Refer Athletes with Psychological Concerns at the Secondary School Level." He served on the writing groups for the NATA "Pre-Participation Physical Examinations and Medically Disqualifying Conditions" position statement, and the "Return to Participation Following Musculoskeletal Injury" position statement. He served on NATA panels on Spearing in College Football, and the Preparedness and Management of Sudden Cardiac Arrest in High School and College Athletic Programs. He also serves on the NATA Committee on Professional Ethics judicial panel.

Mr. Neal has presented at many national, state, and local sports medicine conferences and written articles on athletic training, catastrophic incident preparedness, risk management, and psychological concerns among student athletes for many national publications. He serves on the advisory boards of *Training & Conditioning Magazine*, *Athletic Management Magazine*, and *College Athletics and The Law* publication. He is a subject matter expert for the Human Performance Resource Center for the U.S. Department of Defense.

A graduate of Ohio University, Mr. Neal earned his master's degree from Syracuse University.

Eric F. Quandt concentrates his practice on complex litigation and life sciences. Mr. Quandt is an experienced trial lawyer having successfully tried cases including products liability, pharmaceuticals, medical practice, medical devices, asbestos, and personal injury litigation. His trial experience includes various state and federal courts

throughout the country. Mr. Quandt is a "AV Preeminent" peer review rated by Martindale-Hubbell, reflecting the highest peer recognition for both ethical standards and legal ability.

Mr. Quandt has been recognized as a "Leading Lawyer" in Medical Malpractice Defense Law and Products Liability Defense Law for several years. He was also recognized as an Illinois "Super Lawyer" in 2010.

Mr. Quandt has significant experience in sports medical legal issues and was one of the founders of the Institute for Sports Medicine and Sports Law in conjunction with Northwestern University's Feinberg School of Medicine, Division of Sports Medicine, Department of Medicine, and with assistance from the National Sports Law Institute at Marquette University Law School. Mr. Quandt was one of the two course directors who organized three national conferences with faculty from around the country, addressing medical and legal controversies in collegiate, professional, Olympic and high school athletics.

Mr. Quandt assisted the Big East Conference Sports Medicine Society in organizing "The Clearwater Symposium", a national sports medicine and sports law conference held in Clearwater, Florida. He has represented team physicians, athletic directors and athletic trainers in a variety of claims involving intercollegiate and professional sports.

Mr. Quandt received a B.S. in 1973 and a J.D. in 1976 from the University of Wisconsin-Madison.

James Thornton received his Bachelor of Science in exercise science from Utah State University in 1987. He performed duties as graduate assistant athletic trainer at University of the Pacific in Stockton, Calif., and was awarded his master's degree in Sports Medicine at U.O.P. in 1989. Thornton was then hired as assistant athletic trainer in the fall of 1989 and remained in that position until accepting a job as head athletic trainer/director of athletic training services at Clarion University of Pennsylvania in June 1990.

Mr. Thornton's responsibilities at Clarion University also include being adjunct faculty in the first distance education based athletic training education curriculum in conjunction with California University of Pennsylvania's CAATE accredited program. This program utilizes distance education technology and Internet based learning to accomplish educational criteria. Thornton also performs duties as adjunct instructor for California's Online Exercise Science and Health Promotion Master's Degree program.

Mr. Thornton is a certified athletic trainer by the Athletic Training Board of Certification, and is licensed the Commonwealth of Pennsylvania. He is a certified Performance Enhancement Specialist and Corrective Exercise Specialist by the National Academy of Sports Medicine.

Thornton has been active in the issues that surround the sport of wrestling since his days at Utah State. He has served as the athletic training liaison to the NCAA Wrestling Rules Committee for 16 years. When the unfortunate deaths of three wrestlers occurred in 1997, Thornton served as chair of the Athletic Training Task Force charged with making recommendations for permanent rules changes in weight class management and certification. This weight class certification procedure is now the standard of care for wrestlers at high schools and universities nation wide. As liaison, he is the contact person for all NCAA wrestling institutions concerning questions for weight class certification procedures and rules specific to the medical issues of the sport.

He has served as the district secretary of NATA's District II (NY, NJ, PA, DE), a member of the Eastern Athletic Trainers' Association Executive Board, as well as being a member of the Pennsylvania Athletic Trainers Society Long-Range Planning and Finance Committee. He served a 6-year term as a member of the board of directors of the NATA and was vice president for two consecutive years before transitioning off the board. He previously served as the President of the National Athletic Trainers' Association.

An over-indulgence of anything, even something as pure as water, can intoxicate.

—Criss Jami,

American Author and Lyricist

Today knowledge has power.

It controls access to opportunity and advancement.

—Peter Drucker (1909-2005),

Austrian-American Consultant, Educator, and Author

Higher Education Risk Management:

An Analysis of Risk Management Departments, Risk Management Professionals, and Compensation

| *L. Lee Colquitt and Christine L. Eick, Auburn University, and David W. Sommer, St. Mary's University*

Abstract: This study examines higher education risk management professionals and their compensation as well as characteristics of higher education risk management departments. Data were collected from a 2015 survey of University Risk Management and Insurance Association (URMIA) members. Data on institutions of the respondents are presented first, followed by data on the characteristics of the risk management professionals themselves, and then data on risk management departments. Finally, compensation of higher education risk management professionals is analyzed. In addition to providing summary information on compensation, regression analysis is performed to evaluate the impact of various factors on higher education risk management professionals' compensation.

Introduction

In 2013 the *URMIA Journal* published an article analyzing compensation among higher education risk management professionals. The study also provided insights into a number of other issues related to higher education risk management departments such as job titles, reporting relationships, staffing levels, and areas of responsibility. The present study is a follow-up to that article. Once again, surveys were distributed to URMIA members with instructions that the survey was to be completed by the most senior risk management professional at the college or university. The 2015 survey was modified in some ways based on feedback from those who took the 2013 survey.

The response to the online survey was very good; 176 surveys were completed, compared to 149 in 2013. The analysis below consists of four sections. First, the institutions represented in the sample are described. Second, the characteristics of the senior risk management professionals who completed the survey are described. Third, characteristics of the risk management departments of the sample institutions are presented. Finally, compensation of higher education risk management professionals is analyzed, including a regression which allows us to estimate the impact on compensation of various characteristics of institutions, departments, and risk management professionals themselves.

Characteristics of Sample Institutions

As was the case in the 2013 survey, the institutions represented in the sample are quite varied. Approximately 50 percent of the respondents report being from public institutions, and a slightly smaller percentage report being from private institutions. Between 10 and 20 percent of respondents report being from a land-grant institution, a religiously-affiliated institution, or a campus with at least one medical school. Just under 10 percent of the survey respondents are employed by a community college.

The sample is geographically diverse with four of the six regions representing between 15 and 20 percent of the total sample, and the two other regions representing 12 percent and 23 percent. Also, the sample includes meaningful representation across many different Carnegie classifications, including schools identified as Associate's (12 percent), Bachelor's (12 percent), and Master's (24 percent), as well as the different types of research institutions (12 percent doctoral/research, 18 percent high research, and 20 percent very high research). Finally, the distribution of school size, as measured by student full-time equivalents, is very broad with 16 percent of respondents at schools with fewer than 3,000 student FTEs and 8 percent at schools with 50,000+ student FTEs.

Characteristics of Responding University Risk Management Professionals

The pool of survey respondents was almost equally split between males (51 percent) and females (49 percent). The sample respondents in the 2015 survey are somewhat older than those of the 2013 survey. Like the 2013 survey results, the age distribution is somewhat of a bell curve. However, each of the three youngest age bands make up only about 5 percent of the sample, and the next four higher age bands have 15-25 percent each. A relatively small percentage of the sample respondents are age 65 or older. Interestingly, the average respondent age is 51.7 years for females and 52.2 years for males. This 0.5 year average age difference between genders is considerably less than the 3.1 year age gap in the 2013 study.

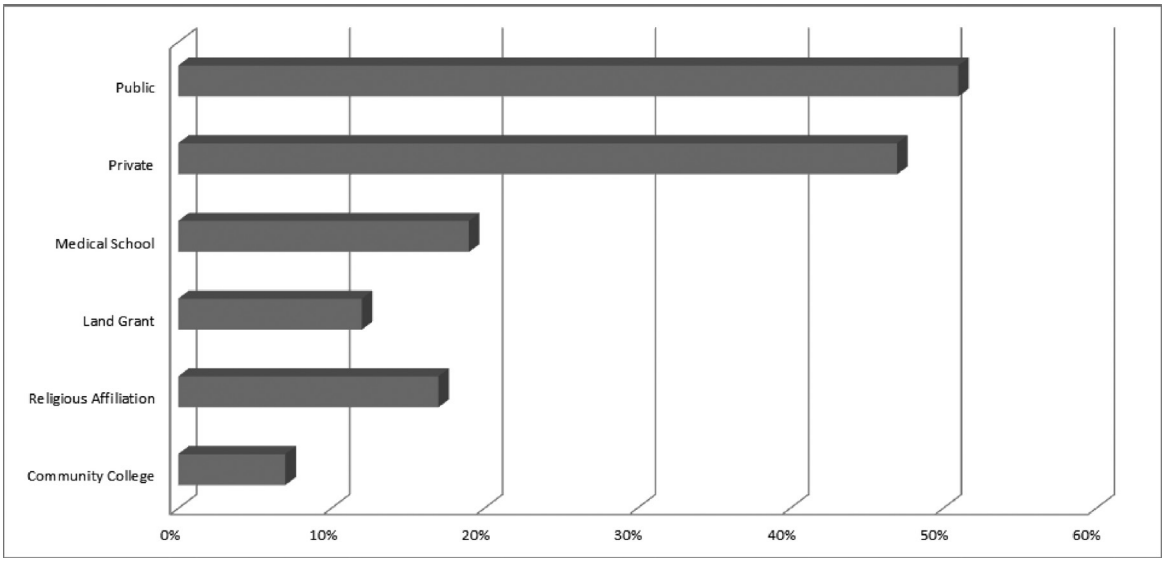


Figure 1: Respondent institutions by type.

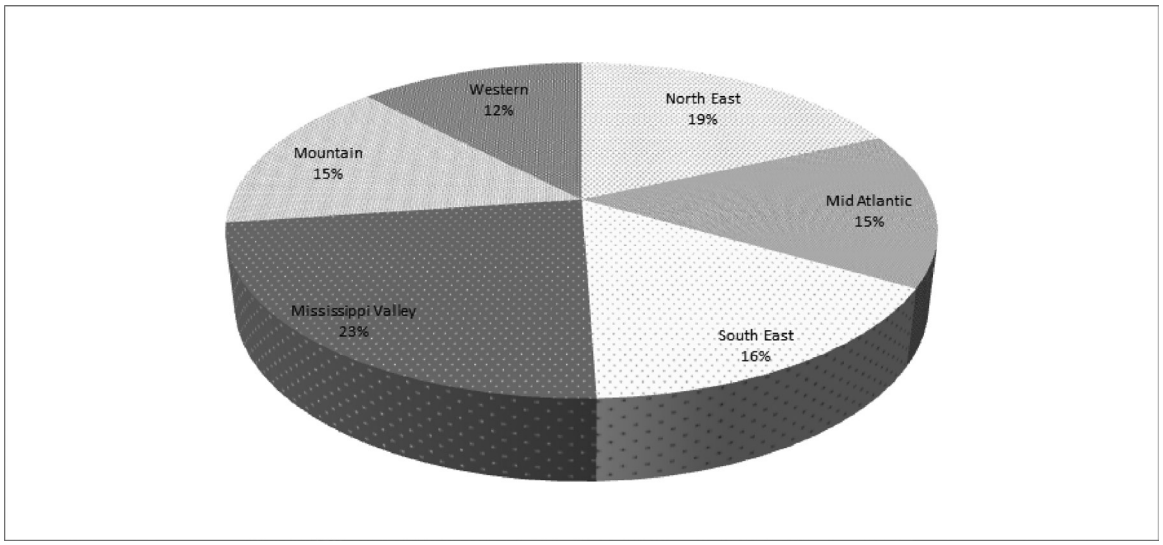


Figure 2: Respondent institutions by region.

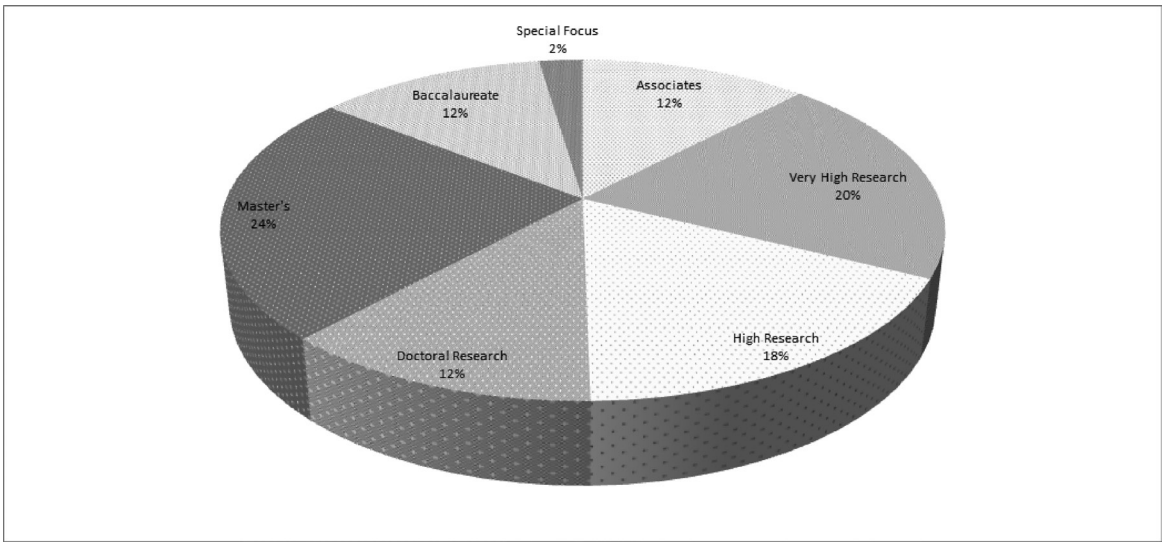


Figure 3: Respondent institutions by Carnegie class.

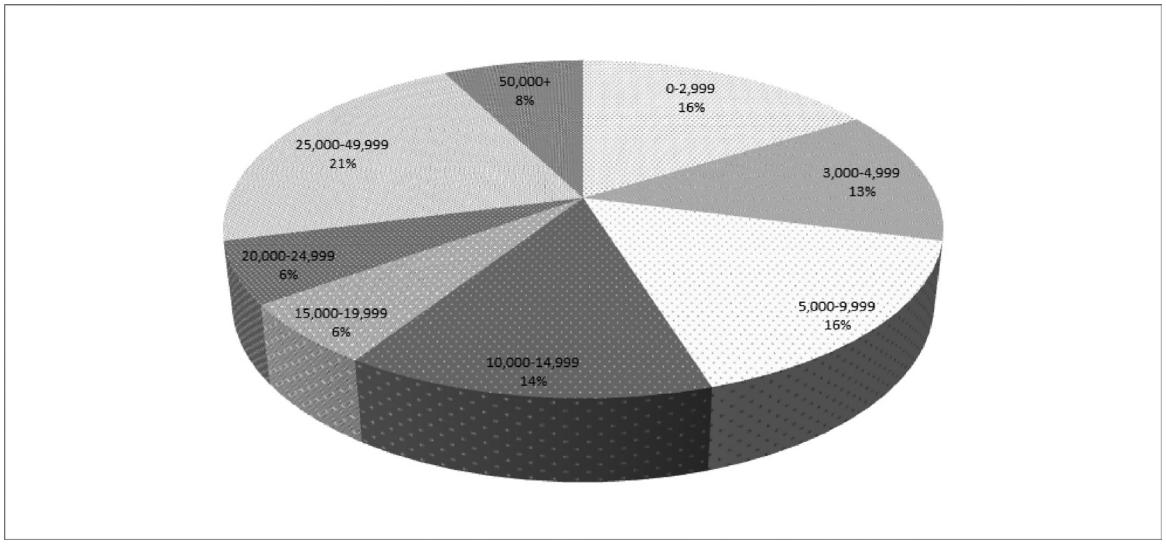


Figure 4: Respondent institutions by student FTE.

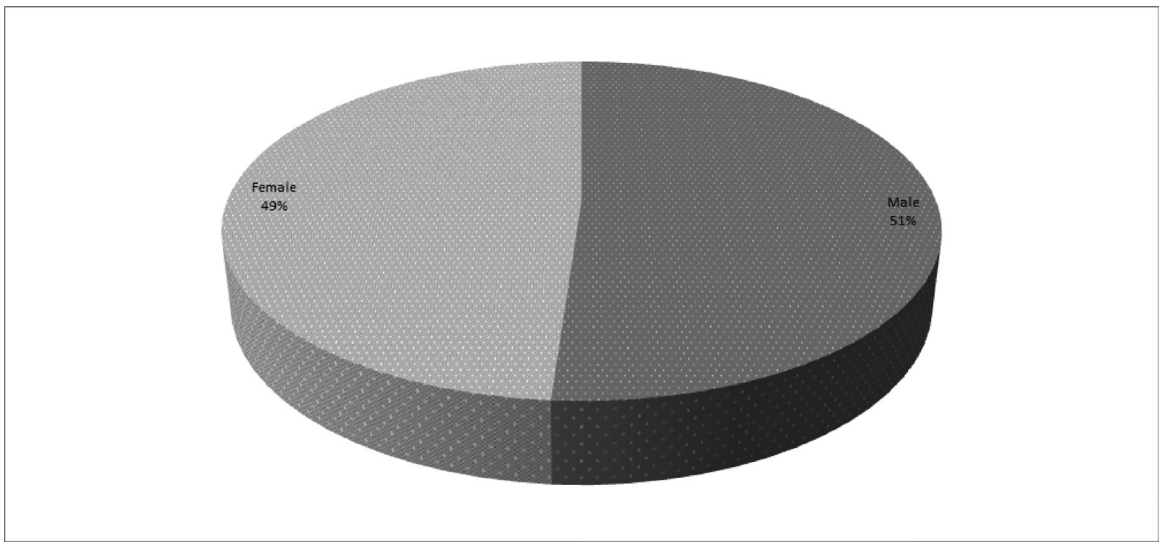


Figure 5: Respondents by gender.

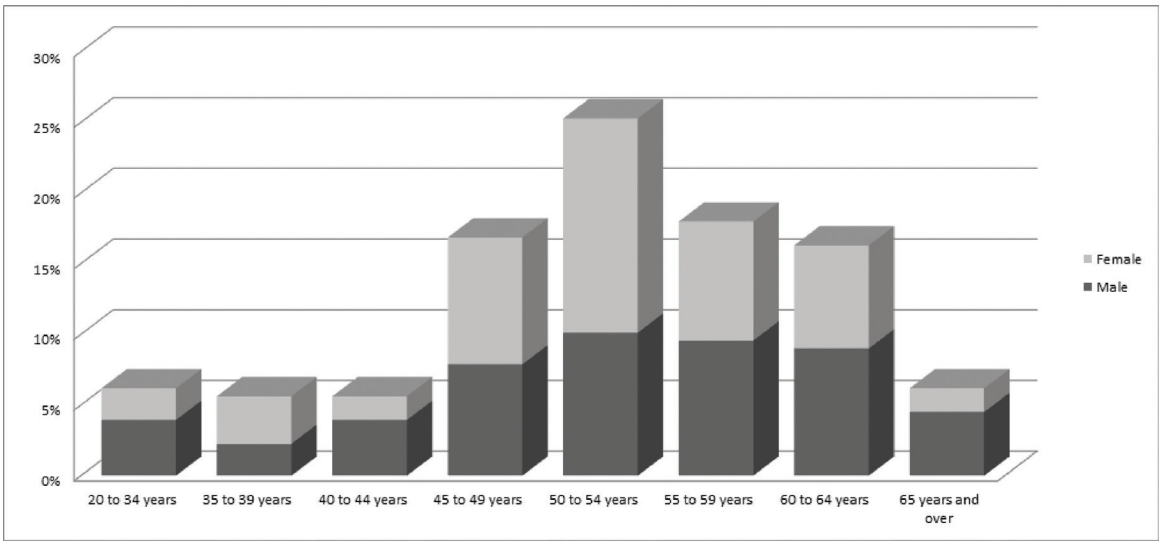


Figure 6: Respondents by age range.

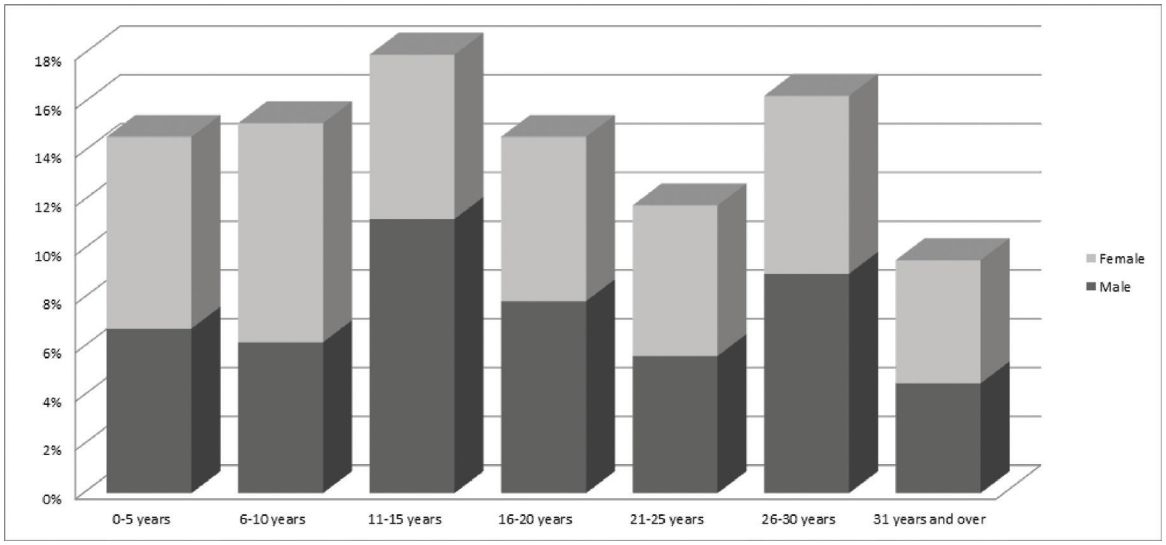


Figure 7: Respondents by years of experience.

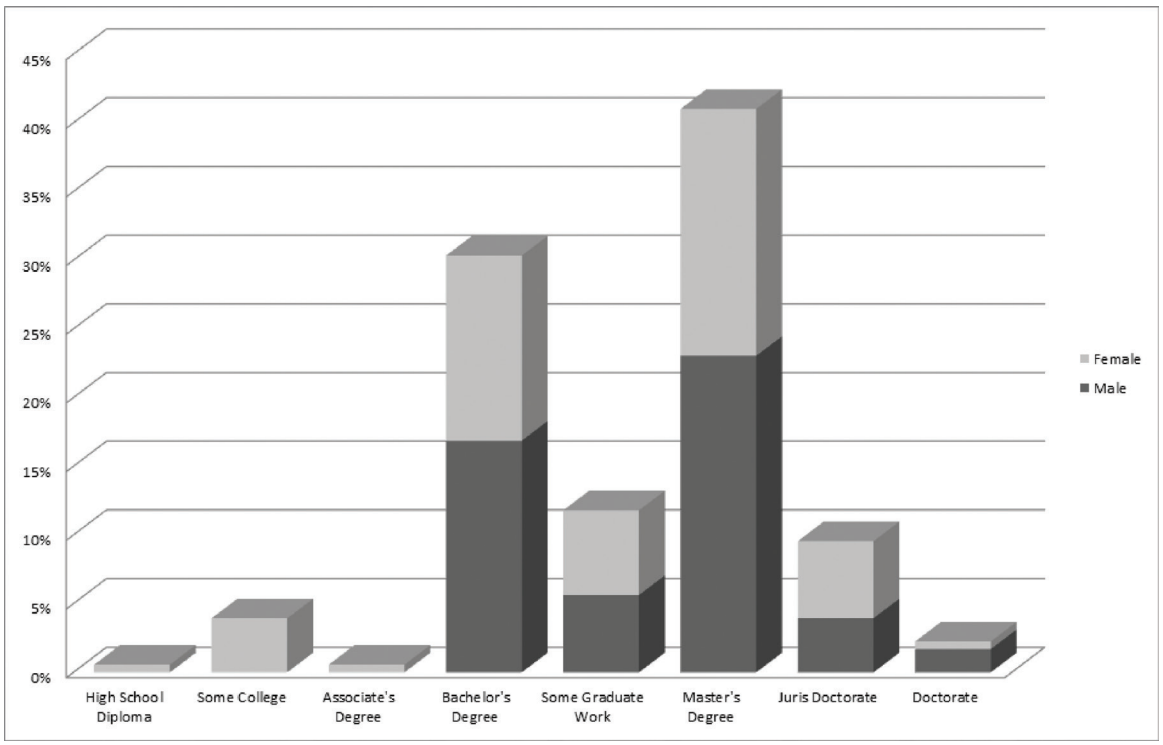


Figure 8: Respondents by level of education.

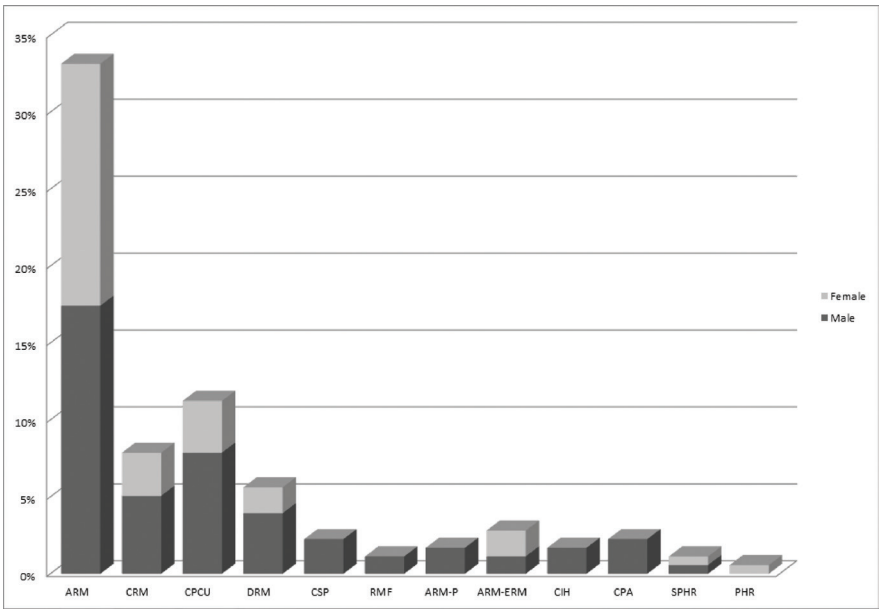


Figure 9: Respondents' professional designations and certifications.

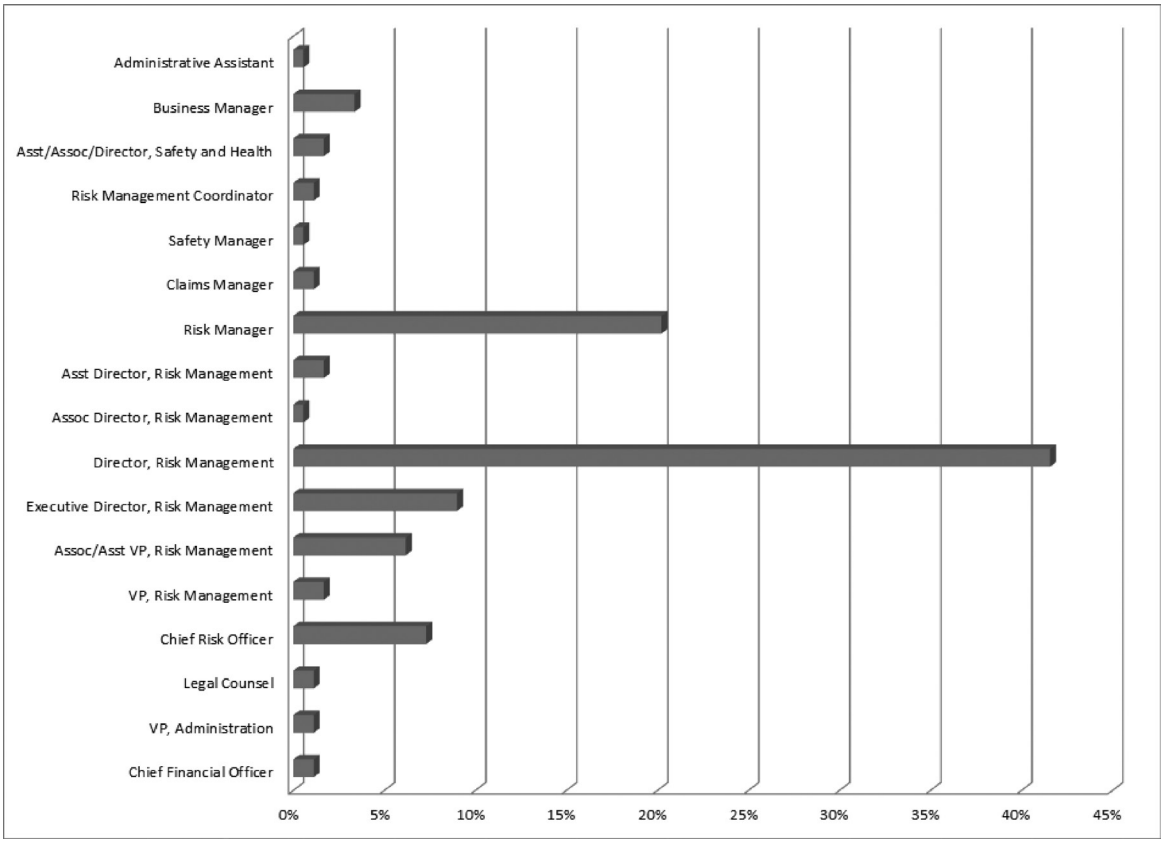


Figure 10: Respondents' job titles.

While there was not an established pattern regarding years of experience in the 2013 survey, the current results for experience are somewhat evenly distributed. Approximately 30 percent of the respondents have 10 or fewer years of experience, and a greater percentage of those with the least experience are females. However, although not shown in the graph, the gap in the average years of experience for males versus females is considerably lower in the current survey versus the 2013 survey. In 2013 average experience was 19.2 years for males compared to 14.7 years for females. This year the averages are 18.0 for males and 17.2 for females.

The survey respondents are generally well-educated with the vast majority holding a Bachelor's degree and approximately 50 percent holding either a Master's degree, Juris Doctorate, or Doctorate degree. Forty-three percent of the respondents hold at least one of the 12 professional designations included in the survey. The most frequently reported designations being held are the ARM (almost 35 percent), the CPCU (just over 10 percent), the CRM (approximately 7 percent), and the DRM (5 percent). Men and women report holding the ARM with approximately the same frequency; 34.1 percent of men and 32.2 percent of women have the designation. However, men report holding the CPCU, CRM, and DRM designations at approximately twice the rate of women.

The distribution of current survey respondents' titles is similar to that reported in 2013 with 62 percent reporting the titles of either "director, risk management" (42 percent) or "risk manager" (20 percent). Interestingly, the number of those reporting the title of "chief risk officer" almost doubled from the 2013 survey, with 7 percent reporting the title in 2015 and only 4 percent reporting it in 2013.

Characteristics of Sample University Risk Management Departments

As was done in the 2013 survey, we collected information about the risk management departments of the respondents' institutions. The vast majority of the risk management departments of the respondents' institutions are small with 65 percent having fewer than three full-time-equivalent employees (FTEs). Those risk management departments with five or more FTEs make up only 14 percent of the sample. There are considerably larger numbers of safety personnel at the sample institutions, with 54 percent having three or more safety FTEs and 17 percent having 20 or more.

In the current survey, the titles of the person to whom the risk management department reports are similar to the 2013 survey, with "chief executive officer," "vice president for business," and "executive vice president" being the most frequently named titles. The number of areas that report to the most senior risk management professional remains rather small for most. Just over 50 percent of the respondents report having two or fewer areas reporting. Only 11 percent of respondents report seven or more areas reporting to the most senior risk management professional. Risk management and insurance and workers' compensation are the two areas most commonly reporting to the most senior risk management professional. Ninety percent or more of the risk management departments manage property/building and contents, vehicle insurance, general liability, professional liability, and crime/employee dishonesty insurance programs. Cyber risk is an area that was not included in the 2013 survey, but given its growing prominence, was included in the current survey. Over 80 percent of the respondents indicate that their risk management department manages a cyber risk insurance program.

Compensation Data

Information was collected on both salaries and bonuses for the most senior risk management professional at each responding institution. Fourteen percent of respondents reported receiving bonuses in the past 12 months with an average bonus of approximately $3,800. Salary and bonuses are combined into total compensation for the remainder of the discussion. The mean total compensation is $103,790, and the median is $97,541 (2013 mean and median were $103,632 and $101,000, respectively.) The average compensation for males in the sample is $110,791, while for females it is $96,628. The ratio of average female compensation to average male compensation in the sample is 0.87, compare to a ratio of 0.84 in the 2013 survey. A lower gender wage gap compared to the 2013 study would be expected given the previously discussed facts that both the age and experience gender gaps are smaller in the 2015 sample.

Of the five most common job titles of the senior risk management professional, the title of "risk manager" is associated with the lowest average compensation, at about

$77,500. Those with the title of "director, risk management" reported average compensation about $22,000 higher than that. Those with titles of "executive director, risk management" or "associate/assistant vice president, risk management" or "chief risk officer" reported the highest average salaries, with "chief risk officers" earning an average of about $148,000.

Average reported compensation rises with age, education, and risk management experience. The difference between average compensation for those holding just a Bachelor's degree and those holding a Master's degree is only about $7,500, significantly less than the $8,900 difference reported in 2013. However, the difference between average compensation for those with a Master's degree versus a J.D. or Doctorate is over $30,000. The relationship between compensation and years of risk management experience is very strong.

Average compensation at research institutions (Doctoral/Research, High Research, and Very High Research) is substantially higher than compensation at non-research institutions, consistent with the 2013 finding. Finally, also consistent with the 2013 study, average compensation for higher education risk management professionals is highest in the Northeastern United States.

Regression Analysis

As was done in the 2013 study, we also performed regression analysis on the compensation data, allowing us to examine the individual impact of particular variables on compensation while holding the other variables constant. Numerous variables were included in different combinations in various regression models. The results shown in the table are for a regression model including all the variables that were ever found to be significant. In addition, a variable indicating whether or not the institution is public is included in order to demonstrate a change in results compared to 2013.

A p-value of less than 0.10 indicates statistical significance for the associated variable. In the 2013 study, the public indicator variable was negative and statistically significant. With the current data, while the public variable still has a negative coefficient, it is statistically insignificant, meaning that after controlling for the other factors in the model, we do not find evidence that compensation at public institutions is systematically different from that at non-public institutions. All of the other variables are statistically significant.

Another change in result compared to the previous study is with the gender variable. In the 2013 study, the coefficient on the variable indicating a female respondent was negative, but had an insignificant p-value of 0.213. For this year's study, the coefficient is negative and marginally statistically significant, with a p-value of 0.097. The coefficient indicates that holding all the other variables constant, female respondents received $7,679 less in total compensation in the past year compared to male respondents.

The final new result in this study is that the variable indicating the respondent has the ARM designation is statistically significant. In the last study, this variable was not reported because it was not significant. The current study's result indicates that the ARM designation is associated with an increase in compensation of over $10,000.

The remaining variables are all statistically significant and are consistent in both sign and significance with the 2013 study. Respondents in the Northeast receive nearly $15,000 more in compensation compared to those in other regions. Those at universities designated as "very high research" receive over $15,000 more in compensation compared to the rest of the group. A graduate degree raises compensation by about $17,000, and each additional year of risk management experience increases compensation by about $850. Respondents in larger risk management departments are compensated more ($3,368 per additional FTE), as are those with a larger number of areas reporting to risk management ($2,090 per additional area).

The R^2 of the regression is 0.441, indicating that the variables in the model can explain about 41 percent of the variation in the reported compensation data. Because the results are based on a sample of only 176 respondents, caution should be used in generalizing the results to the entire population of higher education risk management professionals.

Conclusion

This study provides detailed data about college and university risk management departments and higher education risk management professionals, with a particular emphasis on factors influencing compensation of higher education risk management professionals. Compensa-

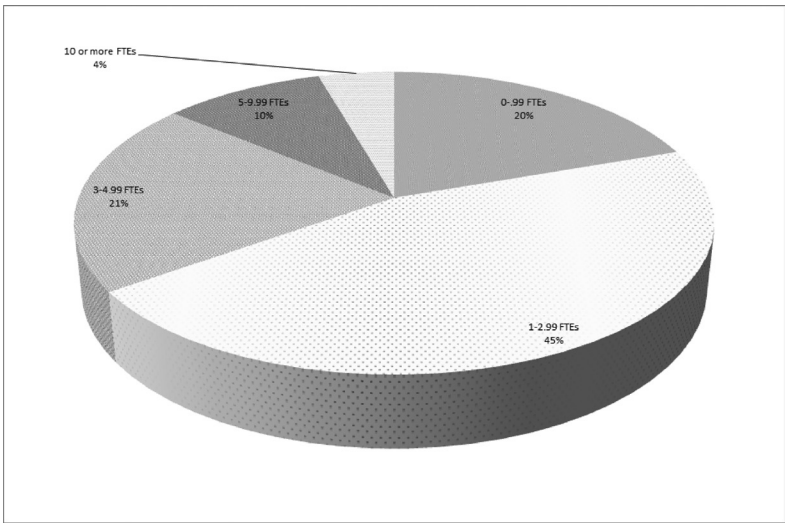


Figure 11: Departments by number of risk management full-time employees.

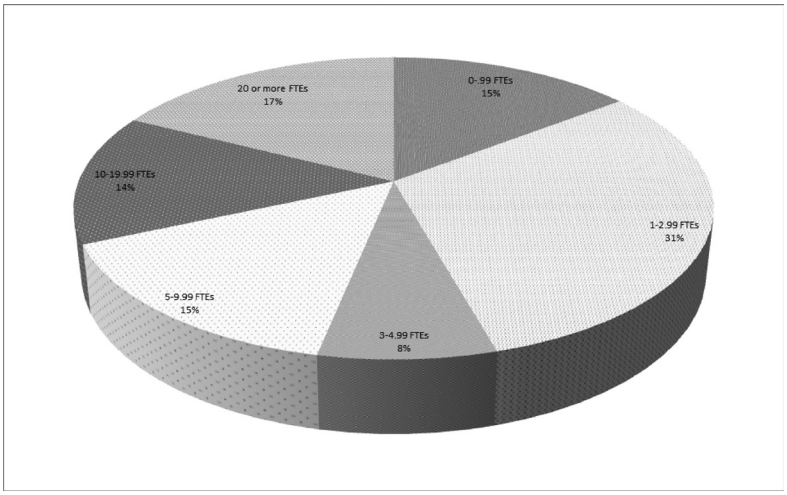


Figure 12: Departments by number of safety full-time employees.

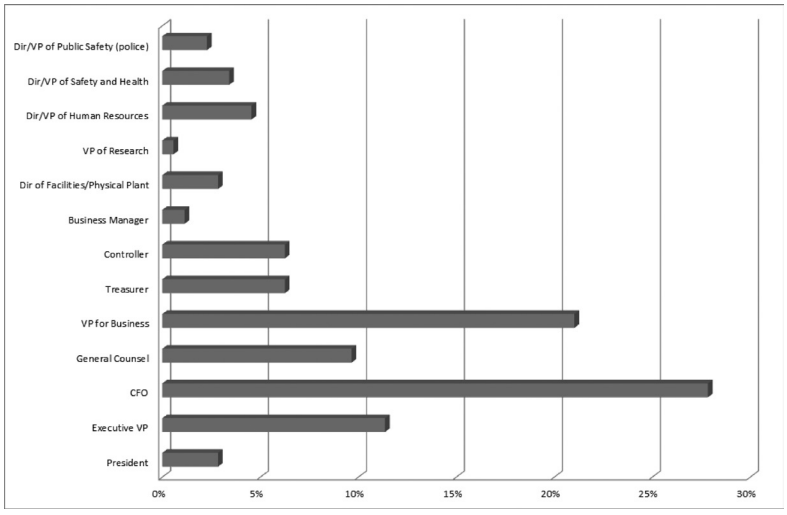


Figure 13: Title of the person to whom risk management reports.

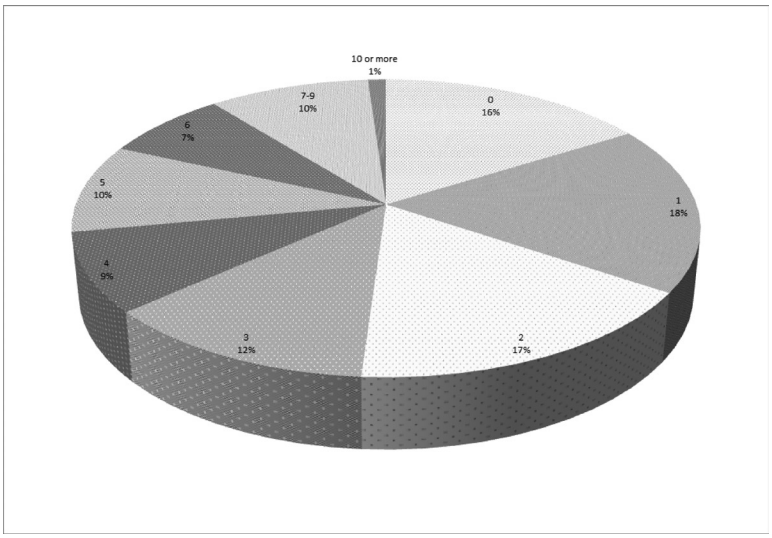


Figure 14: Number of areas that report to the most senior risk management professional.

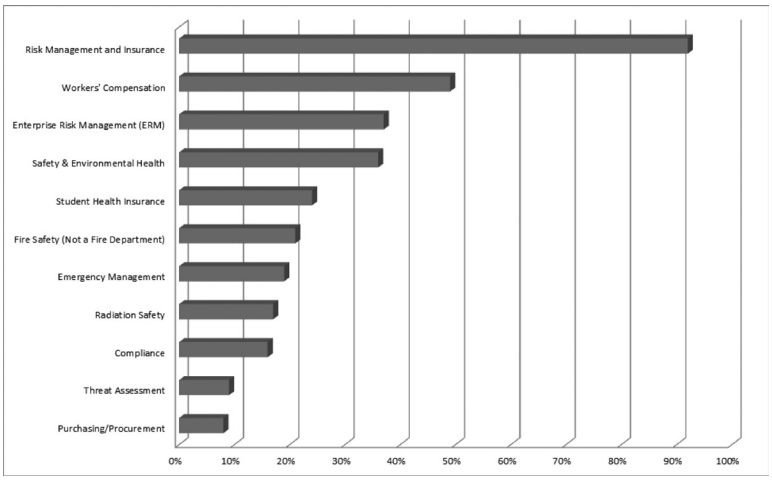


Figure 15: Top 10 areas that report to the most senior risk management professional.

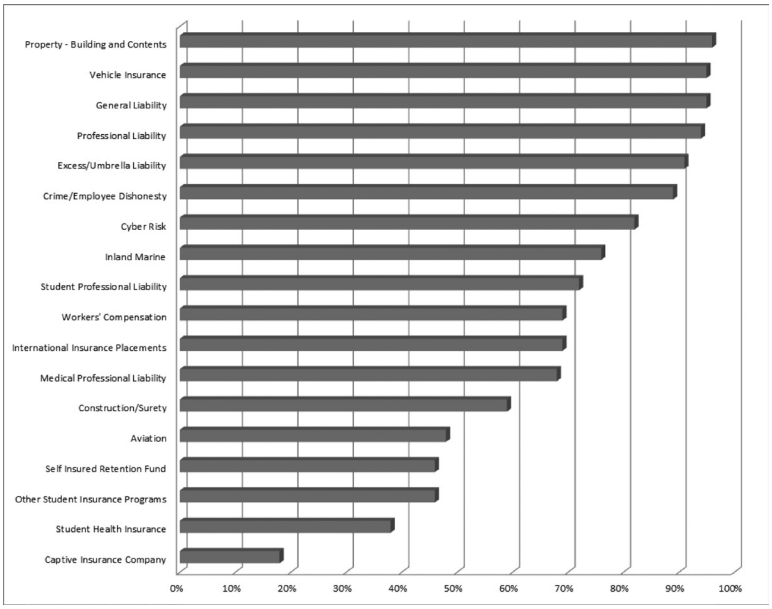


Figure 16: Percentage of risk management departments that manage each insurance program.

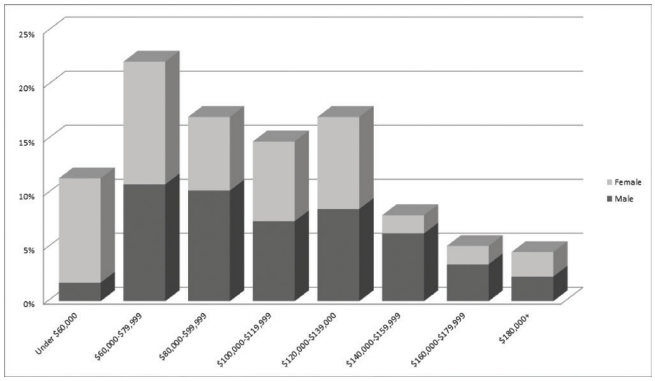


Figure 17: Distribution of compensation.

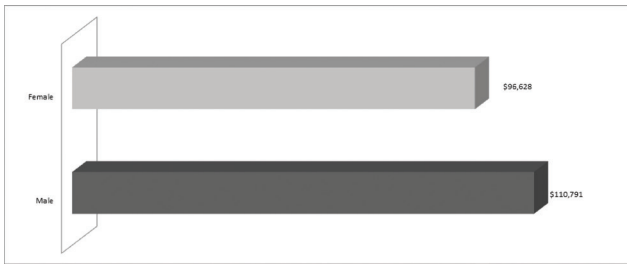


Figure 18: Average compensation by gender.

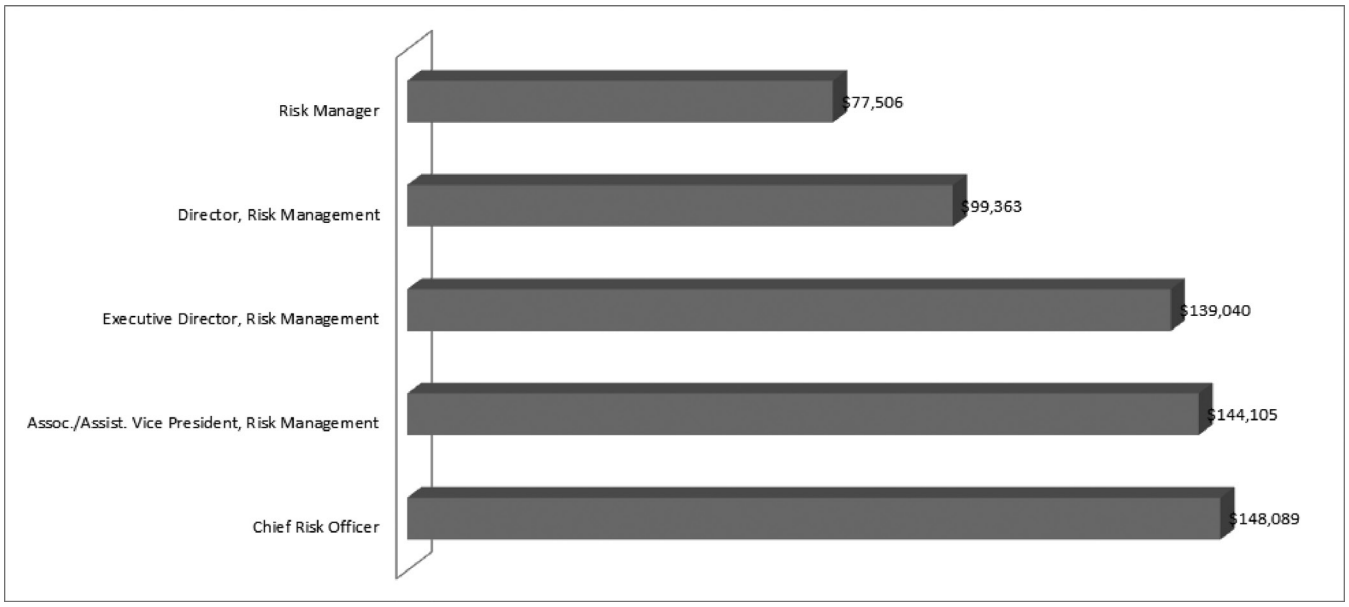


Figure 19: Average compensation for the most senior risk management profession by common job titles.

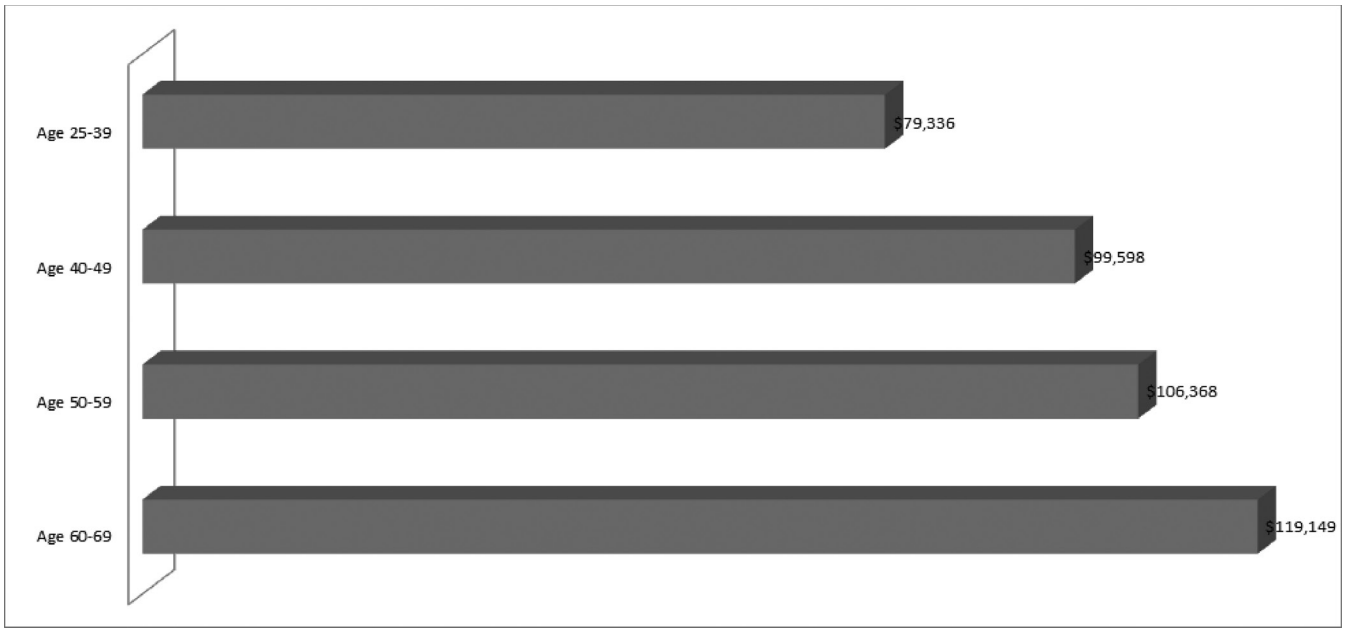


Figure 20: Average compensation by age.

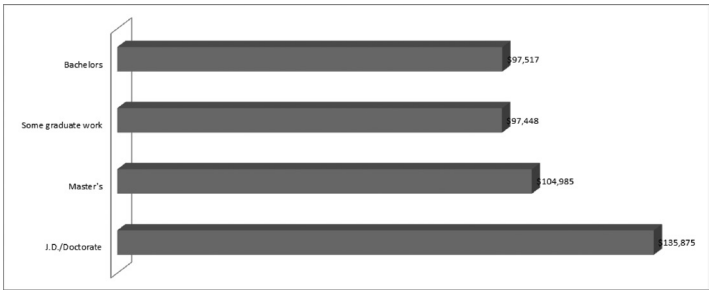


Figure 21: Average compensation by education level.

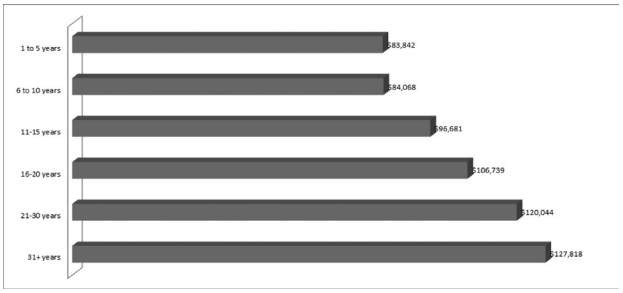


Figure 22: Average compensation by years of risk management experience.

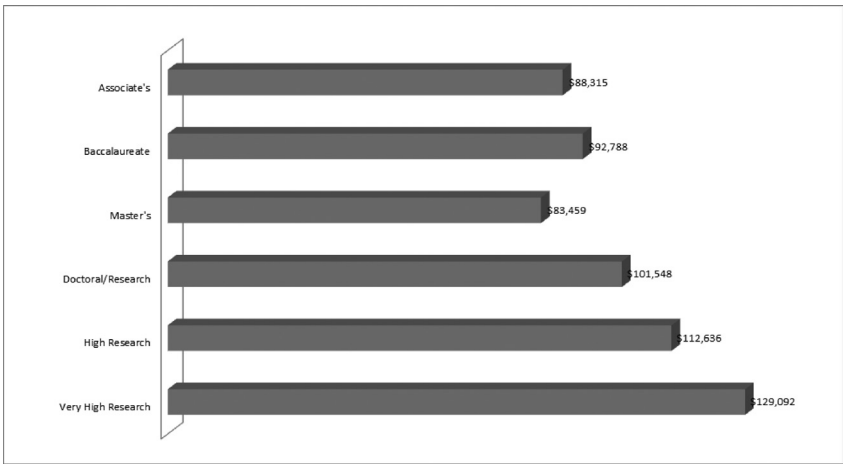


Figure 23: Average compensation by Carnegie classification.

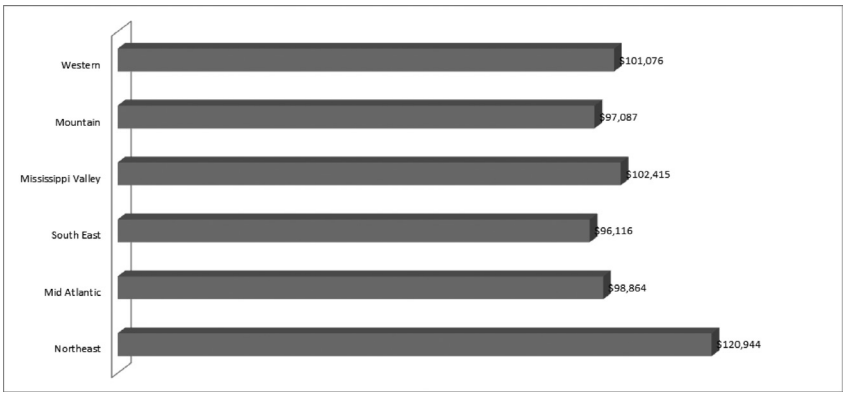


Figure 24: Average compensation by region.

Variable	Coefficient	P-Value
Intercept	59,669	0.0001
Public	-5,517	0.2551
Northeast	14,926	0.0206
Very High Research	15,338	0.0206
Graduate Degree	16,808	0.0001
Years of Risk Mgmt. Experience	846	0.0009
ARM Designation	10,265	0.0510
Risk Mgmt. FTE Employees	2,272	0.0001
Areas reporting to Risk Mgmt.	3,683	0.0001
Female	-7,679	0.0966
$R^2 = 0.441$		

Figure 25: Compensation regression analysis.

tion is found to be statistically significantly impacted by professionals' education and experience. It also varies significantly by region and by the Carnegie classification of the institution. Compensation is also found to be statistically significantly related to the size of the risk management staff and the number of areas that report to the most senior risk management professional. A new result compared to the 2013 study is that having an ARM designation is found to be associated with about $10,000 in higher compensation. Also in contrast to the 2013 study, gender is found to be a statistically significant determinant of compensation. Being a female is associated with $7,679 less in total compensation, after controlling for the other relevant factors in the model.

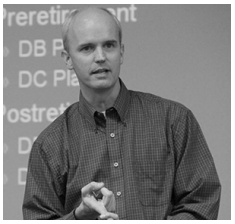
Although gender is found to be a significant factor in compensation, the actual wage disparity between males and females is lower than in the 2013 survey, with a ratio of female to male compensation being 0.87, compared to 0.84 in the 2013 survey. This is likely due to the fact that the experience gap between men and women fell from 4.5 years in the 2013 survey to only 0.8 in the current survey. It will be interesting to continue to monitor the changing demographics and compensation of higher education risk management professionals.

About the Authors

L. Lee Colquitt, Ph.D., is the chair of the finance department in the Raymond J. Harbert College of Business at Auburn University and has been on faculty at Auburn since 1995. He received his B.S.B.A. in economics from Auburn and his M.B.A. and Ph.D. from the University of Georgia. Dr. Colquitt's research has been published in a number of academic and practitioner journals and he has been very active in several academic organizations, serving as president of both the Southern and Western Risk and Insurance Associations. He is also a member of the Risk Theory Society and has been the recipient of research and teaching awards at Auburn.

Christine L. Eick, Ed.D., is the executive director of risk management and safety for Auburn University. She received her B.S. in management with a concentration in safety and health from Clemson University, her M.S. in

risk management and insurance and certificate in enterprise risk management and assurance services from Georgia State University, and her Doctor of Education in higher education administration from Auburn University. Dr. Eick has over 25 years of risk management experience and has served as an URMIA and Atlanta RIMS board member. Dr. Eick is a frequent speaker and has authored several scholarly articles on risk management.



David W. Sommer, Ph.D., is professor and Charles E. Cheever chair of risk management at St. Mary's University in San Antonio, Texas. He holds a B.B.A. degree from St. Mary's University, and an M.A. and Ph.D. from the Wharton School of the University of Pennsylvania. Prior to moving to St. Mary's in 2007, he spent 12 years at the University of Georgia. Dr. Sommer is a past president of the American Risk and Insurance Association, the premier global professional association of risk and insurance scholars. Dr. Sommer has published numerous scholarly articles on a variety of risk management and insurance topics, has co-authored a textbook on risk management and insurance, and has served as an associate editor for multiple academic journals.

Go out on a limb. That's where the fruit is.

—Jimmy Carter,

American Politician and 39th President of the United States

Good management is the art of making problems so interesting and their solutions so constructive that everyone wants to get to work and deal with them.

—Paul Hawken,

American Author and Environmentalist

URMIA 2014 Innovative Risk Management Solutions Award

Waiver Management: Chapman University eWaiver System

Allan Brooks, Chapman University

Introduction

In 2012 Chapman University Risk Management made the decision to deal with the universal frustration experienced by students, staff, and faculty in creating, signing, and storing waiver forms for voluntary participation in activities and events. Over the years we have used either a Word document or PDF template that could accommodate some minor customization, but that did not address all of the various frustrations associated with this process.

I think that most of us understand that the effectiveness of a generic, all-encompassing waiver form is very limited. A good waiver should contain the elements of assumption of risk, waiver of liability, hold-harmless, and indemnification language. To be effective, each form should be a one-off, reflecting the unique element of the subject activity or event.

A good waiver should contain the elements of assumption of risk, waiver of liability, hold-harmless, and indemnification language.

Managing Waivers Across Campus with eWaivers

So, in 2012 Chapman University decided to enlist the services of our information systems and technology (IS&T) staff in the development of an electronic tool. The goal was to create a tool that allowed authorized parties to create a custom waiver that would be reflective of the unique characteristics of each event. What we did was fairly basic, taking the boilerplate wording of our current form and embedding that into a program that allowed certain fields to be custom-entered electronically. Those fields included: (1) Name of sponsoring entity (this ranges from recognized student organizations to university departments to academic departments with a separate category for faculty-led field trips; multiple sponsors can be used); (2) title of event; (3) event start date and time; (4) event end date and time; (5) event locations; (6) and activity risks (this is one of the more critical customizations; this is where the user enters in the hazards unique to their event).

The end result is a final waiver form, or eWaiver, as we call it, that can be immediately deployed.

The next efficiency that we wanted to address was deployment. Each new eWaiver is housed as a unique URL, and this URL is created with the final approval of each eWaiver. As a control mechanism, we have designated certain persons as "submitters" with the authority to create or submit an eWaiver to the system, but not approve it. A more limited number of persons are designated as "approvers." They review the draft eWaivers, edit them if necessary, and then approve them into use. Once that approval is rendered, the unique URL is created, and the system automatically emails that URL to the approver. The event organizers will email the URL in any communication of the event or can insert it in any marketing materials. The unique URL is all that students need to link to the eWaiver, to review it, and to sign it. At that point, the eWaiver becomes a reality, with the electronic signature. The student is automatically emailed a PDF of the signed eWaiver. The system creates a log of all signed eWaivers, specific to each event, and we can login and click down to the details of each signed form.

Signing eWaivers requires that the participant log in to the form using their official university login credentials, which then authenticates their identity. If they are a minor, the system recognizes that status and provides them an opportunity to enter the email of their parent or guardian. The system will then automatically email a PDF of the waiver form to that individual for their signature. They can either sign it and email it back or fax it to our eFax number so we have it in PDF format to attach to the record. We do that by uploading it to the record for that specific event. So, presto, we have all signed waiver forms electronically with no collection or storage of hard-copy forms.

There are times when a hard copy is needed, such as for those events where participants do not pre-register. They can either login from their mobile device or sign a hard copy. Those hard copies are scanned in bulk and uploaded to the record for the event. So while there is some paper at the front end, we eliminate the need to file it by scanning.

Event organizers can log in to the system, click on their event, and produce a full roster that identifies all persons who have signed the eWaiver. This helps in estimating participation and planning for resource needs. The eWaiver also collects emergency contact information which is especially helpful for out-of-area and overnight travel.

We made it especially easy for faculty to create eWaivers for their faculty-led field trips. They do not need to be trained or entered into the system as authorized submitters or approvers. Based on their login credentials, the system allows them to create and approve their own waivers in one step.

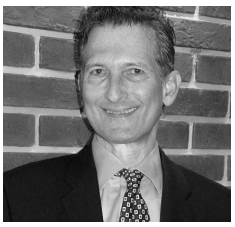
This system has been a great success. The entire university community loves it! We engaged Chapman's Office of Student Life in the early discussions, and they supported the concept from day one. Once we saw how well it worked, we introduced it to faculty as a required replacement for the outdated paper process. That took only one brief meeting with the appropriate vice chancellor.

The system addresses the risk of using poorly-written waivers and the risk of lost waivers due to failture to retain in storage.

The system addresses the risk of using poorly-written waivers and the risk of lost waivers due to failure to retain in storage. We found that many student organizations kept the waivers in their car trunks for a few days then threw them out! That does not happen anymore; these are retained on a network server that receives routine backup. The cost of the project was only that which could be attributed to the time of staff in creating the tool. One programmer worked on it intermittently between other projects, so I do not even have an allocation of hours spent. It was not charged back to risk management, so we do not have a cost to report.

An approach like this can be deployed by schools of all shapes and sizes. For more information, including access to our PowerPoint training material, visit www.chapman.edu/faculty-staff/risk-management/waiver.aspx.

About the Author



Allan F. Brooks, CPCU, ARM, ARe, AU, oversees the Chapman University risk management department and serves as university risk manager. Mr. Brooks is an established industry professional with over 25 years of risk management and insurance experience. He holds a Master's degree from East Carolina University, Greenville, and key industry credentials including the Associate in Risk Management (ARM), Associate in Underwriting (AU), Associate in Reinsurance (ARe), and Chartered Property & Casualty Underwriter (CPCU). Mr. Brooks is a peer in the academic environment with over 10 years of teaching experience at the college level.

Effective leadership is putting first things first. Effective management is discipline, carrying it out.

—Stephen Covey (1932-2012),

American Businessman, Educator, and Author

URMIA Emeritus Members and Their Former Institutions

Robert M. Beth, CPCU, CSP, DRM, Stanford University

Allen J. Bova, MBA, ARM, DRM, Cornell University

Isaac Charlton, University of Alaska

Lawrence Cistrelli, Jr., Ball State University

Ernest L. Conti*, Union College

Mary Donato, ARM, University of New Mexico

Murray C. Edge, ARM, CSSD, WSO, DRM,
University of Tennessee

Charles D. Emerson, DRM*, University of Kentucky

Patricia J. Fowler, CPCU, ARM,
Michigan State University

James R. Gallivan*, University of Illinois

Anne Gregson, University of Rhode Island

Thomas C. Halvorsen, ALCM, ARM, AU, CPCU, BBA, DRM,
University of Wisconsin, Madison

George Harland, Rochester Institute of Technology

Thomas Henneberry, JD, DRM,
Massachusetts Institute of Technology

Alice Horner, ARM, Syracuse University

William Hustedt*, University of Wisconsin

Benning F. Jenness, DRM*,
Washington State University

Michael G. Klein, DRM, Pennsylvania State University

Glenn Klinksiek, CPCU, ARM, MBA, DRM,
University of Chicago

Julie C. Lageson, AIC, ARM, DRM, University of Alaska

Sandra LaGro, Bowling Green State University

Jill Laster, Texas Christian University

Jack Leavitt, MBA, LCPM

Claudina Madsen, DRM, CPSJ Insurance Group

Eugene D. Marquart, DRM,
California State University System

George H. Meeker, ARM, DRM*,
Cornell University Medical College

Linda C. Oliver, Southern Methodist University

William O. Park, MS, MBA, CPCU, ARM, DRM, Northwestern University

Janet Parnell, ARM, University of Denver

William A. Payton, DRM, University of Missouri

Truman G. Pope, DRM, Ball State University

Alex J. Ratka*, University of Southern California

Harry E. Riddell, Princeton University

James R. Roesch, Ohio State University

William F. Ryan, University of Michigan

Martin Siegel, New York University

Donna Smith, University of New Mexico

Stanley Tarr, DHL, DRM*, University of Evansville

Donald Thiel, DRM, University of Michigan

Kathy M. Van Nest, CPCU, DRM, Duke University

Leo Wade, Jr., PhD, ARM, DRM,
University of Southern California

John H. Walker, DRM,
University of Alabama, Birmingham

Jerre Ward, Michigan State University

Robert B. Williams, CPCU, ARM,
The Johns Hopkins University

William J. Wilson, Jr., MBA, JD, DRM,
Howard University

Taryn L. Wiskirchen, Embry-Riddle Aeronautical University

Barbara M. Wolf, California Institute of Technology

Deceased

URMIA President and Past Presidents

2015-2016 **Donna McMahon,**
University of Maryland, College Park

2014–2015 **Marjorie F.B. Lemmon,** Yale University

2013–2014 **Anita C. Ingram,**
Southern Methodist University

2012–2013 **Gary W. Langsdale,**
The Pennsylvania State University

2011–2012 **Steve Bryant,**
Texas Tech University System

2010–2011 **J. Michael Bale,**
Oklahoma State University

2009–2010 **Margaret Tungseth,**
Concordia College (Minnesota)

2008–2009 **Vincent E. Morris,**
Wheaton College (Illinois)

2007–2008 **Ellen M. Shew Holland,**
University of Denver

2006–2007 **Allen J. Bova,** Cornell University

2005–2006 **Mary Dewey,** University of Vermont

2003–2005 **William A. Payton,**
University of Missouri

2002–2003 **Steven C. Holland,** University of Arizona

2001–2002 **Larry V. Stephens,** Indiana University

2000–2001 **Leo Wade, Jr.,**
University of Southern California

1999–2000 **Larry V. Stephens,** Indiana University

1998–1999 **Glenn Klinksiek,** University of Chicago

1997–1998 **Gary H. Stokes,** University of Delaware

1996–1997 **George H. Meeker*,**
Cornell University Medical College

1995–1996 **Linda J. Rice,** Clemson University

1994–1995 **Gregory P. Clayton,**
University of Nebraska

1993–1994 **Murray C. Edge,** University of Tennessee

1992–1993 **Kathy M. Van Nest,** Duke University

1991–1992 **Benning F. Jenness*,**
Washington State University

1990–1991 **Leta C. Finch,** Champlain College

1989–1990 **Thomas R. Henneberry,**
Massachusetts Institute of Technology

1988–1989 **Mary Breighner,** Columbia University

1987–1988 **John H. Walker,**
University of Alabama—Birmingham

1986–1987 **Thomas C. Halvorsen,**
University of Wisconsin

1985–1986 **Eugene D. Marquart,**
California State Universities

1984–1985 **William O. Park,**
Northwestern University

1983–1984 **Alex J. Ratka*,**
University of Southern California

1982–1983 **Truman G. Pope,** Ball State University

1981–1982 **Martin Siegel,** New York University

1980–1981 **Charles D. Emerson*,**
University of Kentucky

1979–1980 **Dale O. Anderson,** University of Iowa

1978–1979 **David N. Hawk,** Kent State University

1977–1978 **James A. White,** University of Illinois

1976–1977 **James McElveen,**
Louisiana State University

1975–1976 **George A. Reese*,** Temple University

1974–1975 **Irvin Nicholas,** University of California

1973–1974 **Donald L. Thiel,**
University of Michigan

1972–1973 **Stanley R. Tarr*,** Rutgers University

1971–1972 **Warren R. Madden,**
Iowa State University

1970–1971 **Robert M. Beth,** Stanford University

1969–1970 **James R. Gallivan,** University of Illinois

Deceased

Distinguished Risk Managers

Recipients are listed along with the university for which they worked when receiving the award.

2014	**Gary W. Langsdale**, Pennsylvania State University
	Steve Bryant, Texas Tech University System
2013	**Ellen Shew Holland**, Oregon University System
	Paul D. Pousson, University of Texas System
2012	**Julie C. (Baecker) Lageson**, University of Alaska
	David Pajak, Syracuse University
2011	**Margaret Tungseth**, Central College
2010	**Barbara A. Davey**, University of Notre Dame
	Vincent Morris, Wheaton College, Illinois
2009	**Donna Pearcy**, The University of Iowa
	Ruth A. Unks, Maricopa County Community College District
2008	**J. Michael Bale**, Oklahoma State University
	Steven C. Holland, University of Arizona
2007	**Allen J. Bova**, Cornell University
2006	**William A. Payton**, University of Missouri
	Linda J. Rice, Clemson University
2005	**Jill Laster**, Texas Christian University
2004	**Elizabeth J. Carmichael**, Five Colleges, Inc.
	Christine Eick, Auburn University
2003	**Paul Clancy**, Boston University
	Mary C. Dewey, University of Vermont
2002	**Larry Stephens**, Indiana University
2001	**Rebecca L. Adair**, Iowa State University
2000	**Glenn Klinksiek**, University of Chicago
	John E. Watson, Pepperdine University
1999	**George H. Meeker***, Cornell University Medical College
1998	**Leo Wade, Jr.**, University of Southern California
1997	**Charles R. Cottingham**, University of Missouri
	Kathy M. VanNest, Duke University
1996	**Thomas R. Henneberry**, Massachusetts Institute of Technology
	Michael G. Klein, The Pennsylvania State University
1995	**James A. Breeding**, Rutgers University
	Donald Thiel, University of Michigan
1994	**Benning F. Jenness***, Washington State University
	Claudina Madsen, CPSJ Insurance Group
	Truman G. Pope, Ball State University
	William J. Wilson, Jr., Howard University
1993	**Murray C. Edge**, University of Tennessee
	Leta Finch, University of Vermont
1992	**Mary Breighner**, Columbia University
	Charles Emerson*, University of Kentucky
1990	**Thomas C. Halvorsen**, University of Wisconsin, Madison
	Stanley R. Tarr*, University of Evansville
1989	**John Adams**, Georgia State University
	Robert M. Beth, Stanford University
	Eugene D. Marquart, California State University System
	William O. Park, Northwestern University
	Lee B. Stenquist, Utah State University
	John H. Walker, University of Alabama, Birmingham

Deceased

The *URMIA Journal* is published annually by the University Risk Management and Insurance Association (URMIA), PO Box 1027, Bloomington, IN 47402-1027. URMIA is an incorporated non-profit professional organization. The 2015 *URMIA Journal* was edited and designed by Luke Zimmer, URMIA, and printing was completed at Indiana University Printing Services.

There is no charge to members for this publication. It is a privilege of membership, or it may be distributed free of charge to other interested parties. Membership and subscription inquiries should be directed to the URMIA National Office at the address above or urmia@urmia.org.

© LEGAL NOTICE AND COPYRIGHT: The material herein is copyright July 2015 URMIA; all rights reserved. Except as otherwise provided, URMIA grants permission for material in this publication to be copied for use by non-profit educational institutions for scholarly or instructional purposes only, provided that (1) copies are distributed at or below cost, (2) the author and URMIA are identified, (3) all text must be copied without modification and all pages must be included, and (4) proper notice of the copyright appears on each copy. If the author retains the copyright, permission to copy must be obtained from the author.

Unless otherwise expressly stated, the views expressed herein are attributed to the author and not to this publication or URMIA. The materials appearing in this publication are for information purposes only and should not be considered legal or financial advice or used as such. For a specific legal or financial opinion, readers should confer with their own legal or financial counsel.

URMIA would like to recognize the following contributors for their efforts in reviewing and publishing the 2015 *URMIA Journal*:

Communications Committee:

Allan Brooks, *Co-Chair*
Julie Groves, *Co-Chair*
Robin Doerr
Deb Donning
Dennis Fleetwood
Diane Gould
Troy Harris
Lorna Jacobsen
Keswic Joiner
Blake Lovvorn
Andrew Lysinger
Samantha McClelland
Sherry O'Neal
Jordana Ross
Marlene Terpenning
Randy Troy

URMIA Staff:

Jenny Whittington, *Executive Director*
Luke Zimmer, *Communications Coordinator*

Yes, risk-taking is inherently failure-prone. Otherwise, it would be called "sure-thing-taking."

—Jim McMahon,

American Football Player

URMIA

UNIVERSITY RISK MANAGEMENT & INSURANCE ASSOCIATION

Presorted
Standard U.S.
Postage PAID
Bloomington, IN
Permit No. 171

If undeliverable, return to:
URMIA National Office
P.O. Box 1027
Bloomington, IN 47402

San Diego

47th Annual Conference Host City | September 17-21, 2016

Front cover photo by Flickr user Rick Seidel flickr.com/photos/56194068@N04/6931786959
Rear cover photo by Flickr user Cavicchi flickr.com/photos/cavicchi/6051808601