

11-2-2016

A Risk Assessment Study at the University of South Alabama Libraries

Richard J. Wood

University of South Alabama, rwood@southalabama.edu

Mary Duffy

University of South Alabama, mduffy@southalabama.edu

Follow this and additional works at: <http://digitalcommons.kennesaw.edu/seln>

 Part of the [Library and Information Science Commons](#)

Recommended Citation

Wood, Richard J. and Duffy, Mary (2016) "A Risk Assessment Study at the University of South Alabama Libraries," *The Southeastern Librarian*: Vol. 64 : Iss. 3 , Article 2.

Available at: <http://digitalcommons.kennesaw.edu/seln/vol64/iss3/2>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in The Southeastern Librarian by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

A Risk Assessment Study at the University of South Alabama Libraries

Richard J. Wood and Mary Duffy

Richard J. Wood is the Dean of Libraries at the University of South Alabama and can be reached at rwood@southalabama.edu.
Mary Duffy is the Asst. Dean of Libraries at the University of South Alabama and can be reached at mduffy@southalabama.edu.

Prior to receiving a memorandum from the Director of Risk Management that the libraries would be included in a university-wide risk assessment study, the authors' only contacts with the director had to do with art works housed in the library and the amount of money kept on-hand at the service desks. We believed that the Risk Assessment Office was primarily concerned with highly vulnerable programs such as the hospitals, pharmacies, athletics, the bookstore, and laboratories. The challenge for us now would be to develop a comprehensive assessment of risks in library facilities and operations from acquisitions and cataloging to circulation, interlibrary loan, reference, and archives.

Although the authors and library supervisors did not have university risk assessment guidelines or policies to base decision-making on, we, perhaps intuitively, considered risks when developing library policies or procedures which involved collecting money at a service desk, ordering and receiving of educational materials and supplies, handling rare books, and picking-up large gift collections from donors. But until receiving the notice that the libraries were included in the university-wide assessment study, the authors had no plans to lead such a study. We quite frankly questioned the need for the libraries to be included in the consultant's study because we collect very little money, have very few chemicals or other hazards in the libraries, and do not put employees or patrons at-risk like hospitals do.

Our question was answered by the consultant at our first meeting. The primary reasons why the libraries were included in the study were due to the monetary value of materials ordered throughout the fiscal year, the value of all materials in the Doy Leale McCall Rare Book and Manuscript Library (McCall Library), as well as total revenue from fines, lost books, interlibrary loans, and copy cards. News headlines about thefts from library rare book rooms contrasted with the common perception that libraries were quiet, safe places where users can locate research articles, find information, or study without putting themselves in danger. Librarians themselves may have entered the field with similar expectations.

Rather, library administrators are likely to believe that the most significant risks they face are natural disasters such as hurricanes, tornadoes, fires, floods, or earthquakes. In coastal areas, for instance, collections may be at risk from high humidity, pests, or other conditions that pose a risk to collections. The threat of active shooters or terrorists who could enter the library with weapons is likely to be

regarded as even more dangerous and more likely to occur in today's environment than natural disasters.

The most common and age-old threat that librarians take into consideration may be theft of materials by patrons. Library staff may not have the inclination, nor the time, to monitor patron behavior. It is easier to believe that students come to academic libraries to study, do research, or read—not to steal books, razor cut articles from bound journals, and so forth. (Those are crimes of opportunity, as well as less prevalent in the digital age.) Nevertheless, security systems for decades have been regarded as necessities, rather than frills by academic and other library administrators to prevent theft. High risk areas such as manuscript collections, rare book rooms, and supply rooms are often monitored by video surveillance systems installed to deter theft, or to track it when it occurs.

Counter measures, on the one hand, may be only as good as the people enforcing, monitoring, or implementing them. On the other hand, few if any counter measures may stop something from happening. Hurricanes, flooding, HVAC leaks, roof leaks, active shooters, and theft occur. Take theft as an example, installing video surveillance systems are not likely to stop determined and knowledgeable thieves from stealing students' laptops. Surveillance systems may, however, be deterrents to would-be thieves. Installing anti-theft measures on works of framed art are no more likely to prevent someone wanting the piece from ripping-off the frame to steal it. Deterrents, by definition, help to prevent or limit damage, theft, and crimes from happening. The authors certainly want to touch on many of the topics such as these, but we primarily want to focus on how we went about assessing risk and developing counter-measures that we found appropriate.

Case Background - The Consultant

In late 2014, the Director of Risk Management notified twenty-three key university administrators that the Marsh Risk Consulting (MRCO) was hired to conduct a campus-wide strategic risk assessment and analysis. The administrators were scheduled to meet with the consultant during the last week of January 2015. The administrative staff included those in the offices of the president, the vice-presidents, the internal auditor, computer services, financial aid, facilities management, housing, human resources, athletics, engineering and design, purchasing, public relations. The Dean of University Libraries and Director of the McCall Library (who reports to the dean) also were scheduled to meet with the consultant.

The consultant's sessions were designed to generate an open dialogue about risks to the University. He defined a "risk" as follows: (a) the probability of threat of damage, (b) injury, liability, (c) loss, or (d) any other negative consequence that was caused by external or internal vulnerabilities, and that may or may not be avoided through preemptive action.

Risks were further categorized as: (a) strategic, (b) financial, (c) operational or (d) hazard. The latter represents a potential source of harm to the health of a person or persons, or to a university asset. An operational risk was associated with an internal, external, system, or employee failure. An employee, for example, who does not comply with a university policy or an environmental or safety law may put himself, or others, at risk. There might be a financial risk to non-compliance as well. Besides thinking of these risk categories, the key administrators were asked to be prepared to discuss two questions with the consultant: What critical risks did you foresee for the activities of your department or field of University operations? In general, what critical risks did you foresee for overall University operations and activities? Another parameter of the consultant's role was to determine what countermeasures the department, school or college took, if any, to mitigate the risks that were cited.

University Background

A relatively young institution, the USA was founded in 1963 in Mobile, Alabama, becoming the first state supported public institution for higher education in south Alabama. The university has grown from one building in 1963 to a sprawling campus in west Mobile, as well as two hospitals and a cancer institute located in mid-town Mobile. Enrollment today tops 16,000 students (head count). With clinics, the physicians and hospitals comprising the USA Health System cared for more than 250,000 people in 2015.

Nine colleges and schools provide quality education in business, computing, arts and sciences, education, engineering, nursing, the allied health professions, and medicine. USA offers 12 doctoral degrees, a Medical Doctor (MD) degree, 32 master's degrees, an Education Specialist degree, and various programs leading to 53 baccalaureate degrees. With over 5,500 employees, USA has a payroll of \$400 million. External contracts and grants are over \$50 million annually. As a charter member of the Sun Belt Conference in 1976, the university fields 17 Division 1 sports teams, including football, baseball, basketball, tennis, soccer, softball, and volleyball.

The rapid growth of USA over such a very short time is certainly the backdrop for the need to look at risks. Realization of the need led to the establishment in the 1990's of the Office of Risk Management and Insurance. Outside of this office, however, risk assessment has not been a formal process, or responsibility, assigned to anyone in most administrative or academic offices with the exception of medical facilities. Risk insurance and claims, for example, are handled by central administration for cost saving purposes.

Other academic administrators at USA have to consider risks and risk avoidance as a normal or natural aspect of decision making. However, in higher education, many university administrators probably rose to their positions based on their academic merit and without the benefit of management education or training, much less risk management training. So, with such diversity of programs and facilities, it made sense for central administration to look to deans, directors, and department heads to assess and manage risks and threats, at least in selected vulnerable programs.

Library Background

From a couple of rooms in the USA's first building (1964), library services and resources have grown exponentially. A large four story facility was built in 1968. When its capacity looked like it would be reached by the early 1990s plans were made to expand by renovating a residence hall near the newly constructed College of Medicine facility for a bio-medical library. By 2000, the Biomedical Library collections were growing quickly, as were the information needs of the doctors, nurses and other medical personnel, so information resources were made available at the Medical Center and Children's & Women's Hospital for use by medical staff.

With donations of many thousands of photographs and negatives and manuscripts, as well as university archives, a separate archives was finally formed in the late 1980s. It is now called the Doy Leale McCall Rare Book and Manuscript Library in recognition of a highly valued collection of early Alabama historical manuscripts, slave records, and books appraised at over \$3.1 million.

Finally, a small collection of business related books and current journals were moved from the Marx Library to the Mitchell College of Business when it was renovated in 2008 for a Learning Resource Center.

Literature Review

The authors searched for similar case studies in the literature. Our literature review revealed a rich bibliography of articles and books about topics such as library security, natural risks, library crime, disaster preparedness, risk assessment, risk insurance, prevention, and the countermeasures that were used to reduce library risks, particularly with respect to protecting collections. We found two very good manuals and starting points for librarians, library managers, and library boards included a manual by Breighner, Payton, Drewes, and Myers (2005) and a guide by Kahn (2008). In each, the authors defined risk identification and management, the process, cost avoidance, loss prevention and control, risk, property valuation, handling claims, and the like

Kahn's (2008) manual included a section on external risks such as plantings, ramps, lighting and walkways and possible counter-measures. His discussion of internal areas such as stairwells, windows, mechanical rooms, and lighting was noteworthy. If the reader were to buy only one

book on overall risk management, Kahn's (2008) library and security guide would be a good choice.

A study by Raffensperger (2010) examined the level of risk based on property and violent crimes using Clery Act data and Uniform Crime Report data. He compared campus crime rates in academic environments with general crime rates. From this data-driven approach, he developed a model for risk assessment, prioritization of efforts, and prevention. However, this article did not help to develop the risk assessment analysis needed for a case study approach.

A book by Shuman (1999) differs in orientation, looking largely at crimes of theft, prevention, policies, and procedures from a broad legal, security, and behavioral perspective and with an eye toward developing a comprehensive security plan. Shuman also discussed electronic security issues and solutions, as well as the future of library security. The author provided a very comprehensive bibliography for those who want to be experts in such matters.

A SPEC kit by Soete and Zimmerman (1999) for the Association of Research Libraries (ARL) surveyed 45 of 122 members and provided a number of documents or forms used to illustrate incident reports, emergency closing policies, bomb recognition points, recovery responsibilities, attempted theft procedures, and many similar procedures or policies regarding use or misuse of computer, theft of library materials, use of fire extinguishers, and so forth. The SPEC kit, however, did not present results, or a methodology, the authors could utilize in preparing for a risk assessment, particularly because USA is not an ARL library.

The American Institute for Conservation of Historic and Artistic Work (AIC) offers any person access to its Risk Evaluation Planning Program (REPP) site questionnaire; just completing it can reveal lacunae in staff and emergency preparedness, policies, procedures, fire safety, and environment.

The National Center for Preservation Technology offers a free online program and easy-to-use template useful for institutions that want to develop a comprehensive disaster plan (dPlan). Its preservation leaflets provides free advice on a variety of preservation topics, as well as links to additional resources.

Methodology

The authors prepared a preliminary outline listing risks by departments or areas as follows: (a) General, (b) Acquisitions, receiving, cataloging, processing; (c) Archives, rare book & special collections; (d) Art and art galleries; (e) Circulation (access services); (f) Interlibrary loan; (g) Loading and receiving areas; (h) Printing and copying; (i) Stacks, office, and other areas; (j) Systems; and (k) Travel. This list served as a checklist to help assure that major areas were not overlooked in the process.

Under each heading, we identified the most obvious risks such as theft, mutilation, ordering library materials for personal use, using library supplies and hardware for personal use, improper use of photocopying machines, and the like. The authors presented this list at the initial meeting (January 2015) of department head and asked department heads to help flesh-out a libraries risk assessment strategy, provide additional input, as well as assist in developing countermeasures in their respective departments.

Library Department Assessment Results

Not having been faced with disasters like Katrina since 2005, library administration and department heads first surveyed risks from theft, unsecured doors, electrical hazards, and other easy to identify risks—the “low hanging fruit”. Seeing too many devices plugged into an outlet or electrical strip, for instance, is easy to spot. USA employees a safety officer and staff who periodically inspect university offices for potential hazards. The safety office staff are always willing to offer advice on counter measures to prevent circuit overloads, fire, or other failures. These staff will also review door and window hardware and provide suggestions as to how to improve room security, access and egress. Such assistance may be far more valuable than the advice offered by a manual or website because the advice is specific to the problem or need. As a result, work orders can be initiated to correct safety concerns, or improve security.

There are more ordinary risks or threats associated with matters not normally thought of as threatening. Such decisions as scheduling library hours of operation, the implementing of new programs and policies, and picking-up gift books from donors are examples. To illustrate one of these examples, we considered a very common issue in academic libraries: extending library hours. At USA, for instance, this matter arises nearly every year during student government association elections, when at least one candidate runs on a platform of extending library hours. By staying open 24 x 7 or 24 x 5 the library staff and users at USA would be more likely to be exposed to increased security risks such as assaults or muggings. If adding a third shift (without hiring additional staff) decreased staffing available for daytime programs, there would be new challenges, particularly when existing staff are ill or on vacation. Hiring student assistants to do the work of classified staff at the circulation desk, for example, is likely to increase mistakes made in taking payments for fines and lost books at the circulation desk. Regardless, library administration on principle should limit risk by imposing stricter cash register and accounting rules to limit opportunities for theft.

A related risk was failing to provide timely and proper training of employees regardless of category (student, part- or full-time staff, professional or paraprofessional). Carefully training and supervising staff responsible for accounts receivable, ordering library materials, or receiving materials should always be regarded as good safeguards against theft. We made sure that staff who order materials are different from those who do the receiving.

We examined whether we allow library staff to use their own vehicles to box and pick-up gift collections at donors' homes or offices. This practice at the very least raises insurance liability questions and could, of course, result in injury, absenteeism and workmen's compensation issues. This is particularly sensitive because many library employees are older and, hence, more vulnerable to back injury. So, library administration now carefully approaches donors when they express interest in donating large collections and try to have the donors be responsible for delivering the gift collection to the library. When this is not possible, we ask student assistants to help or work with university personnel to pick-up the material.

It is the responsibility of library administrators and department heads when making decisions to always consider a diverse array of environmental, behavioral, finance, personnel, and legal factors that pose risks. Such factors are not always obvious at first blush. While it may seem perfectly reasonable, for instance, to approve having food and wine for a reception at the library, university policies should be checked before giving approval. This is because university libraries do not have liquor licenses, but they do have underage students studying who might attend the reception. Another reason may be that university contracts with food vendors who have requirements or policies restricting what is, or is not, permissible.

While unaware of any academic libraries that currently employ metal detectors or armed guards to prevent terrorism or acts of violence, library administrators years ago replaced staff or student guards with security gates that alarm when an item leaves that has not been desensitized. Will library administrators go full circle and once again hire armed security guards in an attempt to protect their facilities from violence or active shooters scenarios? In any case, it is expected that library directors today do realize that active shooters are just as likely to visit the library as they would any other facility on their campus.

This case study is concerned with the counter-measures that the Marx Library took to avoid or limit risk. Library administrators have developed many counter-measures to prevent, or limit, associated risks (See Appendix 1). Among these are security systems, video surveillance systems, lockable supply cabinets, and cash register, all intended to protect library property by limiting theft. In some cases, these same counter-measures may also help prevent or minimize new forms of risk such as active shooter scenarios.

Mobile, Alabama, is at risk of hurricanes for much of the year and has an "Emergency Response and Recovery Plan" (April 2015) in place as a guideline for handling a variety of campus-wide emergencies, including hurricanes. This publication also discusses bomb threats, the university's notification system, hostage situations, hazmat incidents, and other weather conditions. Library employees are asked periodically to study this manual. The Safety Office has planned or surprise drills to help employees prepare for such events. In 2015, for instance, a planned bomb threat in

Marx Library was coordinated between university, city, county and other offices.

The President of USA is responsible for the overall direction of the campus' emergency preparation and response and recovery plan. In the case of a hurricane, therefore, the USA libraries themselves take direction from the President's Council of key personnel. This group makes decisions about cancelling classes, closing campus, directing staff and students to designated safe buildings, and so forth as the situation dictates. After the hurricane, damage is reported by all building facility managers, overall damage is assessed university wide, and appropriate corrective actions (counter measures) are developed and approved to handle reports of damage, re-entry to campus and buildings, resumption of classes, insurance claims, and so forth.

Systems

Data preservation of bibliographic databases is not addressed in the most recent risk assessment by the consultant. Our online catalog is hosted and not managed on site. The vendor of the hosting service provides technical support, including full backups and other data security measures as well as physical security of the server itself.

The list of countermeasures addressed in the Marx Library Risk Assessment does not address in detail violent situations like that of an assault/attack, active shooter or bomb threat, and so on. Those types of events require different responses and will certainly involve local/campus police, fire department and emergency medical support. The reporting requirements for these events are also different.

The first example shows the current risks for the Marx Library Systems department. They include:

- Theft or damage to computers (including thin clients) and related equipment such as printers, scanners, card readers, etc.
- Misuse of computers (including thin clients) such as downloading pornography or sending malware/viruses.
- Hacking of library catalog leading to possible corruption or theft of patron and financial data including fines, purchases, invoice, etc.
- Theft of software.

There are a diverse number of countermeasures that the USA libraries take to limit risk. Use of password protection, authentication, and user verification help protect library computers/users. While a single-sign-on provides a stronger level of protection, the university has not yet implemented this capability.

Video surveillance of high risk areas where there are many computers has proven to be a very useful tool in preventing theft or catching thieves. Video surveillance is useful because few libraries provide trained security staff to actively monitor exits, stacks, and areas that need to be

surveilled. No exception, the Marx Library has very good video surveillance of these areas, but no one is actively reviewing the video feed. Nonetheless, video surveillance systems are expensive and must be updated. Marx Library's first video surveillance system, installed in 2004, was an analog system which required images to be stored on a codec in the library. It was replaced in 2014 by a digital system; now the video can be viewed over the internet from a number of locations, including the university police station. This counter-measure is reactive. In other words, checking a video feed occurs after something happens, to identify the perpetrators, crime, time and date. While not perfect, this deterrent is effective. Because of limited library staff during evening and weekend hours, the system is the first line of defense. Signage is used to alert users to the presence of the video surveillance system. The system, in fact, is more of a deterrent than the presence of library staff because users know it records who comes and goes.

Another reason why theft of computers or damage to them is limited is because computers and computer labs are ubiquitous on the USA campus, including residence halls. In addition, USA students are required to have access to a privately owned computer. The Marx Library's computer lab and public workstations, located throughout the building, offer convenience to students who are more likely to have a laptop or workstation in their room or home.

Replacing higher value computers with thin clients, which are less costly long term, and lack operational capability when disconnected from the network, were also deployed. When installed these devices connect to a central VM server housed in the Computer Support Center computer room. This server delivers access to software and research tools through the thin client. Without access to a similar server, these devices are useless.

Where thin clients are not appropriate, computers are used. Each has anti-virus and anti-malware software installed. While neither software tool is 100% effective, they provide some protection. Additionally, Deep freeze software is installed on all computers. Whenever a computer is rebooted, anything changed or loaded by an ordinary user is deleted and the machine reverts to its original configuration. Anti-theft devices are installed on devices in public areas; they secure computers and thin clients to each other and furniture or other generally immovable objects.

Marx Library's electronic classroom and computer lab are locked unless library student employees or staff/faculty are available to supervise access and use. One equipped study room (ML 123) has a projector and computer. This room is kept locked when not in use, and the key must be checked out (like a book) by eligible users (USA students, faculty and staff). Users are required to return the key afterwards in order to leave and retrieve their ID card.

Although limited, the university does provide some data preservation and protection. Each individual who is employed by the Marx Library has access to a network

drive for data storage. It is an individual's responsibility to backup files and other data.

Circulation Department and Stacks

The staff in the circulation departments of Marx Library and the Biomedical Library are largely responsible for building security and safety because they staff the libraries during all hours of operation. It is important, therefore, that they become very familiar with the USA Emergency Responses and Recovery Plan (2015). All staff are encouraged by library administration to stay familiar with the policies and procedures in the manual because it covers all types of emergencies, including violent crimes, bomb threats, gas leaks, explosions, reporting emergencies, and the campus notification system.

The circulation desks at these libraries is where payments are taken for fines, lost books, copy cards, copying, interlibrary loan payments, and the like. Reducing the number of collection points throughout the libraries has always been a major factor in limiting risk and a practice encouraged by the university's internal auditors. Nonetheless, the university's internal auditor and risk management officer have always regarded the libraries as at-risk--although at low risk compared to the bookstore, or where student tuition and fees are centrally collected on campus.

Most security measures at circulation desks will not stop determined thieves because they know that there is money in the cash register or drawer. Access is limited to full-time staff in order to limit risk. In Marx Library, there is a very secure bank vault that is used to store the cash drawer overnight, but the other libraries do not have this option. The faculty reserves materials are kept nearby as well and include special items, including items owned privately by teaching faculty. Some may be rare and even valuable. Another risk is that fines may be expunged from the ILS or finance systems like banner by trained circulation staff without permission.

Collecting money requires careful handling and training of staff. Even if there is no malicious intent, staff may make mistakes when counting money, making deposits, and the like. Two library staff members are responsible for counting the money, making deposits and locking the cash in the safe at the end of the day. In this situation, such requirements and habits are strong deterrents vis-à-vis only having one person being responsible. We limit handling fines or money to library staff (not student assistants).

Constant supervision of the Circulation area is maintained and a minimum of one staff member is on duty at all times. The libraries print/copy cards are not free. Blank cards must be kept secure and access limited. Cards may be purchased (\$.50) and value added by users at the Circulation Desk. In any case, countermeasures "keep honest persons honest."

Video surveillance systems can reduce crimes of opportunity, but rarely eliminate them. Strategic location of

the cameras help to determine the success of preventing theft. Using a cash register, and enforcing tight procedures, for collection of fines and lost book payments, help limit, but does not totally curtail, the potential for employee theft.

Theft in the public areas of the library like the stacks or large study spaces are most often crimes of opportunity involving unattended backpacks, purses, laptops, or cell phones. A thief can easily spot and take such things, particularly when there are few patrons around who might observe the theft. We addressed this matter in 2003 by installing a video surveillance system. At that time, a university police officer helped to design and install the library's analog surveillance system. We were careful to have every entrance, exit, and elevator under view. The library has a large art gallery, so several cameras were installed in the gallery to protect the art, as well as to assure artists that their works were relatively safe although we do not employ a guard. Cameras with wide angle lenses were installed in some stack areas.

Since the analog cameras were installed originally, the library upgraded to a digital system that stores the images on centralized servers and permit real-time access to university police. Signs are posted throughout the library that video surveillance is being used. Perpetrators caught stealing laptops initially, for example, have mostly been individuals from the Mobile community who intentionally came to steal laptops and re-sell them. Consequently, laptop theft has diminished, so the authors believe that the deterrence value of surveillance systems cannot be emphasized enough.

Most crimes committed in the Marx Library stacks are indeed crimes of opportunity. These include theft of backpacks, purses, clothing, unattended laptops, cell phones, flash drives and of course library materials (books, media, and other materials). Perpetrators run the gamut, including students, staff, faculty, and community members.

Although none of the libraries are in danger of flood waters, there are periodic leaks due to the flat roofs and from heating and air (HVAC) systems. When there are rain storms in Mobile, the circulation staff in Marx Library frequently need to cover book stacks on the top floor, as well as other locations on the first floor. Plastic tarps are kept available for that purpose. Beyond this, however, the university's facilities staff are called to repair HVAC and roof leak problems. That is, library employees are not encouraged or required to make repairs.

Technical Services Department

Technical services at the Marx library is comprised of two sections, Cataloging and Collection Management / Acquisitions. They have different risks: (a) Employees ordering books or materials for themselves through the library, (b) Employees stealing new books or materials before they are cataloged and on the shelves, (c) Unauthorized people accessing staff-only areas and stealing materials or personal items and (d) Injury occurring when moving heavy boxes of materials.

Keeping doors closed, and locking up vulnerable areas and materials, minimizes casual theft as does separating the individual processes and procedures across the sections (cataloging, acquisitions, receiving and mailroom). In other words, taking such countermeasures is a form of checks and balances. No one person is responsible for the entire process. We further limit access by only opening boxes of materials that can be handled in one sitting. If something interferes, and staff are unable to completely process a box, they are required to tape it back up until processing can be finished. Basically this reduces the opportunity for casual theft.

Following strict procedures to maintain a paper trail through acquisitions to cataloging, and promptly stamping materials with the library ownership stamp when received also reduces the opportunity for theft. High value items are kept in a large walk in vault in the Marx Library or in the McCall Archives. Procedures to document access to the vault are also strictly enforced.

Other risks involve activities that may result in injuries. Encouraging staff to use carts or load bearing tools when moving materials also reduces potential injuries. Training on how to properly lift, as well as the safe use of box cutters and other sharp tools to minimize the chance of a cutting injury are important countermeasures.

University Archives

Unlike other library departments, the Doy Leale McCall Rare Book and Manuscript Library (McCall Library) has collections that contain valuable artifacts and materials. When McCall Library was moved into a renovated space in the Marx Library in 2016, the architects, library administration, security office, computer center staff, risk assessment officer, and others reviewed the plans with risk assessment and prevention clearly in mind. Nonetheless, theft or loss of rare and high value items is a constant possibility for a variety of reasons including that materials in this area, are not stamped, barcoded, or tattle taped. While catalog records may establish provenance of an item, or help in identification of items, they are not much help deterring theft. Lack of adequate preservation may also contribute to the loss of these materials.

McCall Library countermeasures are more extensive than for the rest of the library. This department has increased physical security (barriers, locks and limited access) as well as state-of-the-art video surveillance. Again, as there is no staff dedicated to active monitoring of the surveillance system, it is a passive system, good only after a loss or damage has occurred. Other measure include: (a) an independent climate control system to help preserve fragile materials, and (b) enforced use of other positive measures such as cloth gloves and archival boxes, or other storage materials to help reduce deterioration of archival collections/materials. Patrons may only access these materials in a controlled area, a reading room. Additionally, users are banned from using pens and other potentially damaging devices. Access to the archives and collections is

strictly controlled and monitored. Patrons using the reading room are not allowed to bring in bags, briefcases etc. They may bring in paper and pencils.

Other library areas

Marx Library contains two public art galleries that feature exhibits by local and regional artists. The main gallery is located on the third floor and also has twelve glass display cases that often features photographs, crafts, jewelry, and other artifacts. Both galleries, including the display cases, are under video surveillance. The cameras are very visible intentionally. No security guard is provided at any time. In another area of the library, an original Rembrandt etching is on permanent display and the Risk Office required that a specialty lock be installed; it is also under video surveillance at all times. Although the video surveillance system is the only counter measure, there have been no thefts of art to date.

Failure to return interlibrary loan materials has costs and can impact the reputation of the Library. Because material to be picked-up is behind a secured door during evening and weekend hours, there have been no instances of theft. The staff in this department have a very good tracking system as well.

The Marx Library's auditorium contains audio-visual equipment which would be very expensive to replace if stolen or damaged. Anytime this equipment is requested, the requestor is asked to arrive early to have his/her presentation loaded to the workstation ahead of time and learn how to operate the equipment if necessary. Risk is further minimized because the dean's staff carefully monitor requests for reservations. If a group previously caused damage to equipment of the facility, for instance, the policy is to deny future requests.

Marx Library's electronic instruction room contains thin clients and workstations, two flat screen televisions, a projector and an instructor's computer/workstation. To replace or repair this equipment would be expensive. Risk is minimized by limiting access to library instructors. That is, regular university classes are never scheduled in this classroom.

Public institutions are often self-insured; this is an added vulnerability. Self-insurance does not mean that there is a lack of insurance. Rather, being self-insured is a conscious decision to accept risks, quantify them, and create a reserve to cover the identified risks when there are claims.

Most libraries will assume the risk of lost books, computers, supplies, and so on. It would not be cost-effective to pay insurance premiums to cover the cost of most lost books, even though some rare books and manuscripts might be of value to collectors and others. This is the case with many items in the Doy Leale McCall Rare Book and Manuscript Library. One collection alone was appraised in the millions. The university's risk and insurance program would account for such loss.

For example, there are more than 13,000 cellulose nitrate portraits in the Erik Overbey Collection which was acquired in 1978 and housed in the McCall Library in a separate, temperature controlled room. Special containers were fabricated locally to safely move the collection to Marx Library, as well as safely store the nitrate collections. The collection is also being digitized to limit access to this fragile collection.

Conclusions

The purpose of this case study was to identify vulnerable areas and countermeasures to reduce risks. The authors include examples from nearly every department in Marx Library, the main library at USA. However, no one plan can address every possible scenario that may arise. A central purpose of discussing risks and countermeasures with department heads is to bring awareness of vulnerabilities, then develop ways to eliminate or reduce risks. Countermeasures must fit the actual situation that occurs, as well as the budget available to implement them. In any case, identifying risks is the starting point. Risk assessment studies should be done periodically throughout library departments because new risks not only arise, but also new countermeasures are likely to be needed, or old ones adapted. Video surveillance technology, for example, advances significantly every five or so years and cameras will need to be replaced. Analog networks are no longer being supported at USA for instance.

Plan what to do in case of emergency. Decide ahead of time who is responsible for specific tasks in an emergency. Strictly enforce policy and procedures. Train staff how to respond to different types of emergencies. For example, each public service desk is stocked with cans of wasp spray to thwart an active shooter. Wasp spray has a great range and is incapacitating without requiring special skills, but is not lethal.

Identify vulnerable areas and effective countermeasures. These include area/sections that have only one way in/out, as well as those offices and areas that have glass fronts, or those areas that are not supervised (mailroom). Some areas of any library are simply more vulnerable than others. Constant coming and going of authorized staff/workers complicates securing these areas. In the case of the Marx Library, the receiving area requires a key to turn off the internal door alarm and a key to open the external doors into the area. Constant reminders only go so far. Vendors are asked to use the main entrances to the library rather than the receiving area. Such security measures do not solve the problem for university staff working for facilities engineering, or even the Computer Support Center. Have student assistants wear something that easily identifies them such as badges.

General areas, need to be considered for risk as well. Reducing risk is possible by training staff to recognize risks and take action when encountered. Similarly, implementation of video surveillance also helps.

The authors found that fixing or replacing faulty door hardware and locks is an easy, but often overlooked, security measure. For example, there was a large gap between the wood doors leading into the cataloging department. All a thief had to do to gain access was to use a thin object to release the bolt. Installing a metal strip to block the gap now prevents access. So, it is very important to encourage the replacement of faulty door hardware.

Improving communications within or from the library is also important. This might be as simple as the installation of telephones that ring directly to the circulation desk. Such phones could be located throughout the stacks and on all floors. Library administration is determining the feasibility of doing so because it is expected to help reduce risk and also expedite reporting of problems. A related step would be to post emergency telephone numbers at these sites. So, while nearly all students have cell phones to report problems in public areas of the libraries, having telephones and emergency numbers should allow quicker notification and, hence, quicker reaction by police, staff, or other first responders.

Part of the problem of managing risk is getting the information to the right people in a timely manner. The appropriate action is more than a mere phone call. Encourage people to report incidents, share information, log elevator problems, etc. Staff are the first line of defense. Make sure staff know the applicable policies. It may be as simple as locking doors for areas and rooms that are not in use all the time. This may require an investment in new locks. Likewise, consider extending the PA system to all staff areas. People cannot respond to emergencies if they don't know there is one.

Although routines and training might cause complacency, they may also ingrain specific actions in given situations. Routines also help reduce or manage risk. If staff are frightened or stressed, following a routine may allow staff to respond more quickly. In other scenarios, routines may allow detection of problems that might otherwise go unnoticed. Also, checking with the Safety Office on proper procedures for inspecting fire extinguishers, and incorporating any recommendations into library procedures, should insure that they are in working order. Similarly, keeping emergency procedures up-to-date and having an active emergency committee regularly review those procedures, will help to ensure safety. Keeping an inventory of fire extinguishers current, for instance, will help to insure there is an adequate number of functioning fire extinguishers and that they are located in strategic locations. Having functioning fire extinguishers in the right place, however, will do little to reduce risk if staff do not know how to use them. Our risk assessment review led to asking the university's fire Marshall to hold a training session on how to use extinguishers. It was surprising how many employees did not know how. Training, in general, is often the most important countermeasure and way to reduce risks. It is critical that library staff know what to do in an emergency. Besides reviewing procedures and emergency plans, if possible, practice.

Another key element is being able to recognize and distinguish between library users and employees. One way is to provide lanyards or other standard device that identify student/staff workers. Signage will help direct library patrons in the book stacks looking for materials to a safe place. People might not otherwise know where to go, or what to do, in case of an emergency. Examples include, placing evacuation maps throughout the library, or even post QR codes in stacks that will autodial cell phones to the Circulation Dept.

In this day and age, it would be foolish to ignore potentially violent situations. This category includes bomb threats, active shooter situations, fights, vandalism, aggressive patrons, etc. To address a potential violent situation, library leaders need to be aware of, and plan out, what the best response would be (as far as anyone can tell beforehand). At a minimum, there are two Youtube films that can be shown to employees: Auburn University's Active Shooter Response Training (ALICE) and UAPD Active Shooter Video: Avoid, Deny, and Defend. The USA campus police also led a session for library employees and showed a film. Finally, a bomb threat was simulated and coordinated with the police department, the Safety Office, city, county and other offices. Such training should be scheduled periodically so new staff are covered. Library administrators need to realize that this training is especially important for staff employed in the libraries' circulation department who work evenings and weekends.

The authors found that an area of high risk, given recent news headlines, was bomb threats. Realizing that library employees were never trained on how to deal with a bomb threat, the authors decided to implement in-house training with the help of the university police department and safety officer. To mitigate the risk of real bomb threat, a simulation was planned. This included a bomb threat called into an employee at the circulation department. The employee was told to obtain as much information as possible from the caller: background noise, dialects, accents, sex, etc., and inform the police of all this because even something as innocuous as background noises may ultimately help locate the bomb, prevent an explosion, or reveal a hoax. Planning ahead and training staff is the wisest choice. For example, designate a code word, that when used, will alert employees of a bomb threat or emergency.

Another area for employee training is the risk of active shooters. Such situations are different in that there may not be time to call for an orderly evacuation of the library. In some cases evacuation may even put employees and users in even greater danger; they should only evacuate a building if they can do so safely. If they cannot, they may need to hide to protect themselves. Another critical first step is to notify the police. But a call should only be undertaken if the employee is in a safe place and has a phone readily available. If there is no other option but to hide, police advocate piling furniture and whatever else is available to block the shooter. Police recommend fighting back in dire circumstances. Throwing books or other objects at the shooter long enough to distract or disable him

may provide enough time for employees and users to escape. In the event that the situation is happening in another building on campus, the library must be able to secure the building and wait for the police to give the all clear.

Recommendations

Risks in any academic library need to be considered when making decisions. Risks also need to be periodically assessed, particularly when technology changes, renovations occur, or other circumstances warrant. The risk assessment case study presented here occurred because a risk consultant was hired by the university to determine university wide risks. The libraries at the University of South Alabama were included because of a planned renovation allowing the Doy Leale McCall Rare Book and Manuscript Library to move into the main (Marx) library. Another reason was the collection of money for fines, lost books, interlibrary loans, and so forth. In any case, what library administration and department heads learned during this time needs to be applied periodically—perhaps a three, four or five year review using the same methodology.

Many colleges and universities, including the University of South Alabama, have implemented security alert systems to facilitate prompt notification when dangerous situations arise. These systems don't negate the need to plan and train library employees for emergencies in order to protect people, materials and facilities. As problematic as it may be, risk management should not be overlooked. While it is difficult to anticipate the violence someone may do, or to avoid a theft, library administration can, and should, identify areas and implement procedures that take advantage of the library's strengths to prevent theft, or to minimize harm to people, and damage to library materials. Risk assessments may be organized by departments and use department heads to help facilitate them, as well as developing and maintaining procedures and countermeasures to limit risk. All countermeasures are likely to need updating as technology and the availability of products on the market change. Hopefully the information outlined in this article and in resources identified in the literature review will help. Working with safety compliance officers and maintenance staff should not be overlooked. Finally, risk assessment should not be regarded as a task that may need to be checked off but, rather a process that should be employed by library administration to protect the safety of library staff and users.

References

- Angeli, E., Wagner, J., Lawrick, E., Moore, K., Anderson, M., Soderlund, L., & Brizee, A. (2010, May 5). General format. Retrieved from <http://owl.english.purdue.edu/owl/resource/560/01/>
- Breighner, M., Payton, W., Drewes, J. M., & Myers, G. E. (2005). Risk and insurance management manual for libraries. Chicago: Library Administration and Management Association.
- Kahn, M. (2008). The library security and safety guide to prevention, planning, and response. Chicago: American Library Association.
- Raffensperger, T. (2010). Safety and security in urban academic libraries. A risk assessment approach to Emergency Preparedness. *Urban Library Journal*, 16(1): 1-5. <http://ojs.gc.cuny.edu/index.php/urbanlibrary/article/view/1252/1314>
- Soete, G. J., & Zimmerman, G. (1999). Management of library security: A SPEC kit. Washington, DC: Systems and Procedures Exchange Center, Office of Leadership and Management Services, Association of Research Libraries.
- Shuman, B. A. (1999). Library security and safety handbook: Prevention, policies, and procedures. Chicago: American Library Association.
- University of South Alabama: The First 50 Years, 1963 – 2013. (2013). University of south Alabama. Mobile, AL.
- University of South Alabama Emergency Response and Recover Plan. (2015). University of South Alabama, Mobile, AL <https://www.southalabama.edu/departments/environmental/resources/Emergency%20Response%20Plan%20%204.24.2015.pdf>
- University of South Alabama Statistical Profiles. (2014). University of South Alabama. Mobile, AL. <http://www.southalabama.edu/departments/institutionalresearch/resources/FactBook2014-15.pdf>
- University of South Alabama Statistical Profiles 2008-2009. (2014). University of South Alabama. Mobile, AL. USA: A Brief History. (n.d.). Retrieved from <http://www.southalabama.edu/aboutusa/historyofusa.html>

APPENDIX

Risks and vulnerabilities	Countermeasures
Leaks	Initiate a phone tree so key personnel are informed. Pre-position tarps, mops and buckets so they can be easily accessed. Provide list of key campus contacts, with phone numbers/email addresses.
Art works	Consider installing anti-theft devices and video surveillance system when applicable.
Computer hardware and software	Consider installing anti-theft devices and video surveillance system. Consider replacing workstations with thin-clients.
Doors and windows	Inspect locks and repair or replace damaged hardware. Install window treatments to limit visibility of room contents. Periodically inventory keys assigned to staff and faculty. Establish procedures for securing building at closing.
Hazmet (storage & use of chemicals)	Consult with university safety office about proper storage, use, policies, etc. Periodically inventory storage closets so it is known what Hazmet materials are stored properly in the library.
Natural disasters and emergencies	Follow university emergency response and recovery procedures and policies for power outages, fire, flooding, weather, bomb, terrorist, hazmet, and similar incidents. Otherwise, follow best practices. Have basic supplies on-hand for immediate recovery.
Theft	Consider range of measures from installing signage, anti-theft devices/locks and video surveillance to purchasing lockable cabinets.
Violence	Protect patrons and staff. Contact campus police. In extreme cases, evacuate the building but only if possible to do safely
Bomb threat	If threat is phoned in, get as much information as you possible from the caller. Contact campus police. Initiate evacuation of the library. People should be moved away from the building to safe areas.