Navigating the Complex Claim

Lessons Learned and Moving Forward

2019

Gallagher

Insurance | Risk Management | Consulting

"To improve is to change; to be perfect is to have changed often."

—Winston Churchill

"If this were true, the insurance industry would be perfect, too."

—Anonymous

Participants and Presenters

The following individuals generously participated in an in-person think tank meeting on the subject of complex claims in February 2019. While this report does not necessarily reflect the views of any attendee, presenter, institution or organization, it generally reflects the contributions of the participants and, in many instances, a coalescing of concepts. As the disclaimer below indicates, the report does not purport to establish standards or best practices of any kind.

Think Tank Participants

- **Karen Cornelius,** Risk Manager, Loyola University Chicago
- **Chauncey Fagler,** Executive Director and Chief Risk Officer, Florida College System Risk Management Consortium (FCSRMC)
- **Luke Figora,** Senior Associate Vice President, Chief Risk and Compliance Officer, Northwestern University
- **Karen Kruppa,** Director Risk Management, Suffolk University
- **Cheryl Lloyd,** Associate Vice President and Chief Risk Officer, University of California, Office of the President
- **Craig R. McAllister,** Executive Director, Office of Risk Management, University of Miami
- **Amy Mendez,** ARM, Director of Risk Management, The Claremont Colleges Services
- **Nancy Pringle,** Executive Vice President, Human Resources, Ithaca College
- **Chad Tindol,** Vice Chancellor and Deputy GC, University of Alabama System
- **Stacy Youngdale,** Associate Director, Risk Management, The University of Texas System

Gallagher Staff

- **John McLaughlin,** Senior Managing Director, Higher Education Practice
- **John Watson,** Executive Vice President, Higher Education Practice
- **Elizabeth Carmichael,** Consultant and Contributing Editor
- **Paul Davis,** Esq., Area Assistant Vice President, Gallagher Cyber Liability Practice
- **John Ergastolo,** Area Executive President, Management Liability Practice
- **Eric Pan,** Area President, PNP | Managing Director, Higher Education Practice
- **Paul Pousson,** Managing Director, Higher Education Practice

Preface

We are often asked how we choose the topic for our think tanks. Are the topics submitted by clients, do we conduct a brainstorming session to choose between competing ideas, or does a topic easily rise to the surface as the issue of the day? Over the years, all three of these processes have been used to choose a theme for a think tank.

The idea for the 2019 think tank came from our underwriting community; more specifically, it came out of a conversation we had with senior underwriters from one of our leading excess liability markets. Let me provide you with some context.

Beginning in 2018, the long-promised shift in the insurance market began to take hold. For the first time in many years, insurance rates were increasing and seemed to be gaining momentum. While rates were increasing in most industry sectors and across most coverage lines, a more dramatic change was occurring in the higher education liability market. Not only were rate increases significantly outpacing market changes, but insurance companies with a long history of underwriting higher education accounts began leaving the market. Other carriers decided to reduce the limits they would offer, while still others began to introduce coverage restrictions and, in some cases, added full-blown exclusions for exposures such as traumatic brain injury and sexual abuse and molestation to their policy forms. Higher than average rates, reduced capacity and more restrictive coverage—higher education had entered a hard market.

Why the dislocation? Was it poor loss experience? Certainly, there had been a number of large high-profile liability claims in recent years, but these seemed to be isolated incidents. Traumatic brain injury is worrisome, but proactive steps had been taken to manage that risk. Was the evolution of Title IX claims or burgeoning losses related to the #MeToo movement the root cause? Or was it an amalgamation of these factors and industry experience that lead to this apparent dislocation in rates?

We needed to dig deeper. In the later part of 2018, we met with our key insurance markets to better understand their underwriting positions. It was during one of these meetings that the topic for this year's think tank was hatched. One of our leading excess liability markets had recently advised that they would no longer accept new higher education accounts. When asked why this dramatic shift in appetite, the senior underwriter responded "Higher education institutions have a pattern of making compound claims management errors when confronted with a complex claim. They turn serious losses into catastrophic events." While not as clearly articulated, we found that this concern was shared by other excess liability (general liability (GL)/directors and officers (D&O)) underwriters.

We can choose to debate the veracity of these perceptions, but we thought our time would be better spent learning from each other how best to prepare for and respond to a complex claim. The panel of risk management practitioners who worked with us in developing this paper have had experience managing complex claims/events. They shared insights, lessons learned and new practices adopted after working through a challenging occurrence. Their insights were invaluable in helping us explore steps that can be taken to prepare for the possibility of a complex claim and actions to take in response to a complex event.

This paper is not intended to be a manual on how to manage claims, but rather an exploration of how risk managers can help their institutions to be prepared to handle complex claims when they arise, and to learn from them organizationally after they occur. Our hope is that readers will also use some of the examples outlined here to help their institutions adopt policies and procedures that will minimize the risks involved in a complex claim.

John McLaughlin
Senior Managing Director
Higher Education Practice
Gallagher

Table of Contents

The old saying goes, "Those who do not learn from history are doomed to repeat it."

I. Executive Summary

As indicated in the preface, this paper is designed to help risk managers prepare their institutions for the added risks of incurring and managing complex claims. It hardly seems fair—just having the underlying loss is bad enough, but now we learn that there are unique risks and responsibilities associated with the management of that loss.

It helps to first know what makes a claim complex. Section II outlines several common elements that can appear in complex claims regardless of the subject of the claim, that is, whether the claim is for property losses or arises from a cyber event, or liability. These are sorted into two categories: (1) examples of situations where the complex nature of the claim or occurrence is readily known and (2) claims that only might morph or grow into complex claims if conditions change or the claim is poorly managed. These are both challenging, but it is likely the second possibility that underwriters were referring to in their expressions of concern about complex claims. Readers will want to spend some time in this section for a good grounding of the issues.

The next section summarizes how to generally prepare for the complex claim. These are the basic strategic elements that can serve as the foundation of every institution's claims management process and, if implemented, will help set the stage for success in managing all claims.

Stories about risk and loss are one of the most important tools that a risk manager can use to communicate to others about risks. This paper is no different, so we have used three hypotheticals to illustrate how a claim may either emerge as a complex loss or grow into one. These stories are gathered into Section IV, Unique Elements by Type of Claim, and are intended to help institutions keep from turning somewhat difficult claims into complex claims. Readers will want to come back to these sections more than once. Bulleted lists can be turned into claim management checklists to aid teamwork in responding to claims. Shared stories may correspond to situations that have occurred on your campus.

Section V, Emerging Areas of Complex Claims is a look to the future. These are areas where our participants believe we all have increased exposure for new types of complex claims. Many institutions are already facing claims arising out of these emerging risks.

Finally, we sum up with the classic risk management practice of continual improvement by highlighting what risk managers can do for claim preparedness after the response to the loss is finished. By "finished" we mean, for example, that all litigation and appeals are over, that the institution is back up and running after a property loss, or that all accessed record holders have been notified and given protection resources.

The appendices are resources for materials, and we encourage you to explore them. If you come across any great resources that are not listed, please let us know!

II. What Is a Complex Claim?

Think tank participants began our discussion looking to identify characteristics associated with a complex claim. In many situations, the complexity of an event or claim is readily apparent. However, in some situations the complex nature of the event or occurrence is not fully realized until further investigation is undertaken; in still other situations, complexity is an offshoot of how we responded or failed to respond to an event. In all situations, participants agreed that early identification of a complex claim situation or event was essential to improving claim outcomes.

Complexity in a claim is not necessarily defined by the dollar value of the loss. Complexity may arise or increase in a loss due to a failure of multiple systems that would otherwise have prevented or mitigated the loss, or from a cascading series of interrelated events. (Example: A water pipe breaks in residential housing, causing water damage on multiple floors; the cleanup uncovers asbestos in old floor tiles. Months after project completion, students begin complaining about headaches and bronchial issues they believe are caused by mold buildup as a result of recent water damage.) Our think tank participants grouped complex claims into two basic categories: (1) situations that are immediately identified as a complex claim to which appropriate resources are allocated and (2) situations that grow or morph from what seems like a straightforward claim into a complex claim.

Examples of situations where the complex nature of the claim or occurrence is readily known include:

- **A very high dollar amount claimed or lost** can create complexity in and of itself. Disputes between the insured and insurer are more common in large loss scenarios, and parties involved in large liability disputes may be less likely to settle. These types of claims are often driven into litigation, which is inherently more complex than a settlement process.
- **High-profile individuals, programs or research** can also complicate a claim, very often because the institution is vested in containing the matter to avoid embarrassment for the parties involved and reputational risk to the institution. One outcome of this can be delays in reporting.
- The event involves the **unnatural loss of life** of someone on campus or for who the institution has some level of responsibility.
- **An active shooter or terrorist** event that occurs on campus or impacts employees or students regardless of where the event occurs.
- A claim of **sexual molestation of a minor** is very likely to be complex.
- **Sexual abuse, sexual assault, rape and serial sexual assault** claims carry heightened concern. New claim reporting requirements instituted by some insurers have added to the complexity involved in the investigation and reporting of these events.

It is harder to identify claims that only might morph or grow into complex claims, but we were able to identify a number of claim or event characteristics that apply to this group. This second category of occurrences or events may not generate the same immediate awareness as those referenced above but would suggest the possibility of complex claim issues. Characteristics common to most types of these claims include:

- **Multiple parties (defendants and/or claimants)** involved in the loss create complexity because their interests may not align. While it is common for institutional employees to be named in a claim or suit, don't overlook third-party defendants, such as contractors to the institution. The defense team may be coordinating efforts with a completely separate defense team and insurer. Claimants are seeking their best outcome and may want to resolve their claim against the institution separately from other defendants. Where there are a lot of claimants, they may decide to come together as a class action, creating a different type of claim, but one that essentially has one claimant plus the lawyers. **Cyber liability** claims, such as a data breach, are very likely to involve parties from multiple states, with those state laws applicable to notice and liability. Even **property claims** can have multiple claimants, such as a residence hall fire or multiuse building with employee and faculty offices.
- **Federal or state agency involvement** in a claim can increase its complexity. In **liability claims**, if the wrongdoing or harm arose out of a violation of law, rule or regulation, agencies may be conducting separate, simultaneous investigations to civil cases underway. In addition to civil damages, there may also be fines and penalties imposed. Similarly, in cyber claims, investigations into the matter by the FBI, Homeland Security or other federal agency can create significant difficulties for the institution in responding to the matter, particularly if there are governmental agency-imposed secrecy requirements. Complex, large **property claims** may be covered in part by FEMA or the state's version of FEMA, adding in layers of documentation, reporting, timing and other requirements to effect recovery.
- **Extensive discovery or complex valuation of loss or claim** can tie up institutional personnel and consultants as they scramble to produce documentation in support of the matter being litigated, whether it is a **liability, property** or **cyber** claim. The cost of producing documents, whether paper or electronic, can be very expensive and time-consuming and a direct drain on normal productivity. This can be especially true in claims alleging negligent behavior spanning multiple years and **losses involving research,** where live animals or biological specimens may have been bred for hundreds of generations, and valuation of the lost research is highly subjective.
- **Complex insurance issues** that arise out of a claim can make the campus claims response team feel like they are under siege from all sides. There are four key areas of insurance complexity.

  a. **Questions of interpretation and application of policy terms** may result in the claim being all or partly denied because the insurer does not believe that the coverage either is provided in the insurance contract or because the insured failed to meet the policy terms required to access coverage (e.g., timely reporting of the claim).

  b. Some claims arise from activities that occurred over more than one policy period, sometimes over many years. **Multiple insurance periods** may mean multiple deductibles in order to access additional limits; they may also mean that there are different policy terms for occurrences that take place over multiple years. A subset of this can be difficulty in finding old insurance policies, or evidence of a policy can result in a denial of the claim.

c. **Claims that may trigger multiple types of policies** are also likely to be complex. It is not uncommon for a single occurrence to trigger multiple types of insurance coverage. For example, **liability** claims may involve both the general liability and educators legal liability/D&O/management liability policies. A **cyber** loss may involve crime, property, general liability and even educators legal liability/D&O policies. **Property** claims can include environmental liability, boiler and machinery, and inland marine floaters; policies can have sublimits on coverages like flood, quake, time elements and others that can complicate recovery.

d. In cases involving multiple defendants, **individual defendants may have their own policies.** A doctor's malpractice policy might respond together with the institution's liability policies, or a contractor's insurance may respond in cases where there is the potential for shared liability.

- **Exposure to reputational risk** may result in increased complexity. Public statements in response to the claim may worsen the reputational damage if not carefully constructed. Runaway social media misinformation and/or attacks may be difficult or impossible to control, and may add to the complexity of managing aspects of the loss. The institution is often walking a fine line in deciding whether to get out in front of a story versus simply responding before it goes viral. Further, the impact on the institution's brand may be a strong consideration in settling a complex issue before it becomes a public display. While this is more common in liability situations, it can occur with property losses, where the institution is embarrassed by the loss having occurred because of negligence or failures on the part of management.

Many complicating factors are unique to liability losses, including cyber liability. Since liability encompasses many types of claims, a few examples are listed here:

- **Complicated testimony regarding causation** arises most often when the subject matter is highly technical and nuanced. This may be more of a defense team concern than a risk management concern, but it is useful to note that good and appropriate documentation and record keeping can help with the investigation and defense of highly technical claims, such as those involving intellectual property or damages caused by pollutants.
- **Procedural complexity, including legal venue and choice of law**[1] can greatly complicate a claim, particularly if the legal venue and choice of law are in different states than the defending institution's state. One participant described a situation where the university was sued in a different state, under the laws of a third state. The venue proved to be the most important factor in the case because the climate was fairly hostile to the educational institution. The legal team recommended that the matter be quickly settled, because the case would go against the school regardless of the merits of the defense. International claims can add additional dimensions to the litigation of a matter, including time differences, travel, differing legal concepts and being the outsider.
- **Punitive damages** can create complicated questions regarding whether to defend or settle the claim, as well as disputes with insurance carriers regarding their contribution to settlements if punitive damages are not covered or covered at lower limits.
- **Geographical dispersion of parties or property** involved can sometimes create complexity in a claim because of the possibility of multiple legal jurisdictions or venues. Another issue can be the

[1] The state of California defines complex civil cases as being in need of special handling or "more intensive judicial management" (see http://www.occourts.org/directory/civil/complex-civil/fact-sheet.pdf, which includes mass torts and class actions) and has a special court assigned to manage these cases.

physical difficulty in bringing the parties together for mediation or hearings.

- **Complex or uncomfortable subject matter** often contributes to **delays in reporting** situations that might create a claim. Sexual misconduct and abuse are examples of this — people do not report because they may be unsure of what happened, embarrassed or ashamed of what happened, or not know where or how to report such a matter. Claims involving intellectual property rights, patent infringement and allegations of antitrust may involve complex legal concepts that result in hesitancy to report. Delays in reporting will always worsen the claim, not improve it.
- **Complex substantive law** is a factor in the liability claims that higher education faces. Substantive law defines the rights and responsibilities under civil law. For example, in a negligence claim, the substantive legal issues can include:
  - The duty to protect others
  - The failure to exercise a reasonable standard of care
  - Proximate cause (what ultimately caused the loss)
  - Actual injury

Higher education has often found itself on the forefront of substantive law, starting with *Mullins v. Pine Manor* in 1982, a seminal case establishing that colleges have a duty to protect their students against foreseeable criminal acts of third parties.

Sometimes it is clear that an event will lead to a complex claim but not always. Failure to perceive the complexity of the event/occurrence and take appropriate steps can turn seemingly simple events into complex claims. Much of our paper will be devoted to processes that institutions can adopt to help reduce the potential that events will turn into complex claims.

In the next section, we will look at ways that the risk manager can help ensure the smooth handling and optimal outcome of a complex claim. By engaging the institution's leadership and management teams in a discussion of what constitutes a complex claim, and helping lead the development of a complex claim policy, the risk manager can prepare the institution for what think tank participants called the "inevitable complex claim."

It almost goes without saying that, if a claim is not reported to the insurer promptly, the claim will become more complicated. All liability policies have some type of provision requiring the prompt reporting of occurrences involving certain types of injuries, sometimes referred to as the "deadly sins." In addition to creating a contractual reporting requirement under the policy, these deadly sins provide valuable insight into the types of events/injuries that insurance companies believe can lead to a complex claim. See the appendix for a higher-education-specific list of events or incidents that typically require prompt notification to insurers.

III. Claim Preparedness — What the Risk Manager Can Do Before a Loss

As previously mentioned, the underwriting community was concerned about what they perceived as uneven claims management practices followed when higher education institutions were confronted by a complex claim or event. Issues identified by underwriters included:

- Supervisors or department heads discounting initial notice of an inappropriate behavior or claim
- Failure to thoroughly investigate claims or keeping the investigation at the department level without notification to risk management or legal
- The institution attempting to manage the claim internally before reporting to the insurance carrier due to reputational concerns
- The incurring of significant legal costs prior to reporting of the claim
- Failure to utilize carrier-provided crisis public relations resources
- The use of nonapproved law firms
- Failure to use or fully consider defense strategies available to the institution
- Decisions to settle losses without consultation with their insurance carriers

Claim preparedness can help institutions avoid these missteps.

Our think tank participants acknowledged that, once a lawsuit has been filed and reported, most of the work in managing the loss is handled by the legal defense team. Risk managers are more often involved in claims that are not in litigation, especially when the institution has large deductibles and self-insured retentions, or operates its own captive. However, when we considered some of the complex claims that have recently been in the news, we agreed that the most important steps an institution and a risk manager can take are usually before a claim ever happens.

- **Make sure that all supervisory staff know what constitutes a claim or reportable incident** and the office to which it must be reported (the receiving office). This is especially critical on issues like sexual assault, harassment, child abuse and discrimination claims, but it is not limited to liability matters. In a decentralized environment, managers may not know to report property losses or cyber losses. Institutional policies and procedures that address these financial events should be explicit regarding reporting protocols, and there must be a clearly defined and communicated process to ensure that the risk manager receives notice of all claims. This means that supervisory staff may need to be repeatedly trained on applicable policies and procedures. Training or reminders need not be long or complicated and can be delivered in a variety of ways.
- **For potential complex claims,** the office responsible for handling the claim should gather an appropriate group of individuals (a SWAT team) to determine what the institutional response should be, based on whether or not they believe this is or could morph into a complex claim. See the next section for suggestions on who might be on your SWAT team for different types of situations.

It has been hypothesized that some of the serial sexual abuse cases in higher education that we have seen in the news evolved into serial situations because institutional employees did not recognize abuse, know what a reportable incident was, nor how to report it. It has been suggested or alleged that, in other instances, someone in the institution may have had knowledge of the sexual misconduct situation but the reports were not shared with risk management, or initial reports were not properly investigated, and the claims were not reported to underwriters in a timely way. From these instances, it can appear that the first impulse of many is to protect the institution's own people or interests when such matters appear in an isolated situation. The delays caused by such impulses can lead to offenders being able to repeat their offences over longer periods of time or against more victims. Delays in reporting can result in litigation over coverage if underwriters allege that policy terms and conditions were not followed. The complexity of claims may be increased due to the inclusion of new, additional victims. It is these failures to promptly react that creates the enormous increased severity.

Understanding how your institution responds to claims through the collection and development of metrics on claim reporting and management can aid in the pre-claim process. More information on this idea is in the section Section VI, After the Loss.

- Claims reporting essentials
  - » Identify your institution's reporting thresholds. These will vary from institution to institution, as to the level and type of incident that is reported, based on the type of coverage involved, the levels of retained loss and reporting provisions in affected policies. With limited exceptions, most policies require insureds to report actual claims either immediately or on a consistent periodic basis. See the appendix for a suggested list of reportable incidents. Define claims for all potential reporters. Here is a common definition: "Any written notice from a person or entity that states an intent to hold the institution or its agents responsible for harm done to them or others by the institution or someone it is legally responsible for (employee or agent)."
  - » Identify who gets trained on reporting. Be sure to include the Office of Student Affairs, Athletics, Human Resources, Provost's Office, Title IX Coordinator, Campus Police, Health Services (including Athletics Health Services) and key supervisory staff at a minimum. Check your policy wording to ensure that all positions identified as designated reporting officers are informed of this responsibility, and are trained on the institution's reporting process and the insurance policy obligations for timely reporting.
  - » Consider who gets the reports. Depending on the size of the institution, this may vary or be escalated depending on the nature of the claim or incident. For example, the Title IX Coordinator may receive all reports of sexual misconduct, put these into a bordereau and send it off to underwriters to meet a notice requirement. Those incidents may then be filtered into categories such as no action, internal investigation, external investigation and criminal investigation, with investigations and criminal investigations being reported to counsel and the senior leadership of the institution.
  - » Identify any groups or departments that are resistant to reporting because they think they have the internal expertise to handle the situation. This presumption of expertise is one of the most difficult things to combat and

can often result in botched investigations, delayed reporting and denied coverage. This issue may need to be addressed by senior leadership if risk management does not have the necessary clout.

  - Don't neglect Campus Police as a reporting source. They may have certain restrictions depending on their state agency, but should be able to fully report on situations that need to be reported to insurers. Health Services is another report source that may have professional standards or legal restrictions on what they can disclose, but they should be required to report certain incidents within these limitations (e.g., child abuse).
  - Remember the importance of onboarding new executives—keep track of turnover, and ensure that they know and understand their responsibilities as soon as possible.
  - Consider making incident reporting an institutionwide policy and procedure—who reports what to whom and when—and make failure to report a disciplinary event.

One way to engage in this process is to do a review of past claims to see how the process actually went, and to create a flowchart of those matters where the claim management went well. It's like taking a forensic history of claims to analyze the institution's practices and identify the best ones for future claims. These can then be shared with response teams and used to drill or practice, similar to emergency response drills.

- **Know your insurance coverage and read your policies.** While the courts may have the final say in coverage interpretation, the better the risk management staff and legal understand what is expected of the coverage, based on policy language, the better positioned the institution will be to take full advantage of its insurance. It is important that legal and risk management have a clear understanding of important provisions within your policies before being confronted with a complex claim. On delivery of your insurance policies, we recommend including your insurance broker/consultant in a review of key policy provisions including but not limited to:
  - Coverage triggers
  - Claim reporting responsibilities
  - Defense provisions
  - Key exclusions
  - Hammer clauses
  - Sublimits
  - Crisis response provisions, if any
  - Other insurance clauses

In addition, this discussion should include a review of how your insurance portfolio fits together. For example, which policies are designed to work together and may require dual notification in the event of a claim? Who are the reporting officers for different policies? What are some potential gaps in coverage? Identify various policies that could be triggered from a single occurrence (GL and excess liability policies, GL and educators legal liability policies, property and cyber policies, etc.) and discuss defense provisions in the various policies. Think tank participants agreed this type of session is very helpful in grounding those with interest in the institution's insurance program on some key provisions governing how coverage responds.

In addition to careful review of your insurance portfolio, participants also suggested the following:

- **Keep track of the claims,** including when they were reported to insurers. Develop your systems in advance of the claims. Options range from sophisticated RMIS systems for large institutions to Excel spreadsheets and a tickler system for smaller institutions. Some policies will have aggregate limits or retentions, and it will be important to understand what claims have previously impacted the policy prior to the complex claim.
- **Get to know your assigned adjusters,** if you have them, especially if you have frequent claims. It can be very helpful to have all claims assigned to a single adjuster or adjusting team, so that communications are consistent.
- **Get to know your institution's communications team** and build a partnership with them. If crisis communications coverage is available to the school through its insurance products, make sure that your communications team is aware of the coverage, knows how to access it, and understands the value this external resource brings to the institution. They should also know to contact the risk manager as soon as they access the coverage.
- **Records management** may not be well organized, so institutions will want to build this reality into their claims management approach by having a good understanding of current records locations and the architecture of their data systems. Know also that stored data may not always be accessible, or it may be very costly to access stored data, if the data storage format is obsolete.
- **Know your carrier-approved outside counsel** and who should represent the institution for different types of claims. Sometimes, on high-profile losses, an institution's board or president will want to be represented by a law firm based on their national reputation. Consider having discussions in advance of a loss to ensure that the board and president understand coverage limitations with respect to choice of counsel, which in some cases requires carrier approval.

- **Identify your institution's sacred cows —** those units, events, activities or people who are so embedded into the culture of the institution that they are, or believe they are, exempt from risk management or compliance controls that apply to others. It can be difficult for a risk manager to get traction on these types of situations that may be above their governance level, but have the conversations anyway. Complex claims may be lurking here.

- **Crisis/emergency response planning and drilling is necessary.** In addition to drilling on hurricanes, fires and active shooters, consider having a short drill with senior administrators on what would happen if a claim came to the institution alleging child abuse, or if a single claim of faculty-to-student sexual misconduct turned into a #MeToo with multiple students reporting incidents publicly over a period of months. All you have to do is look at the daily news for multiple examples to turn into discussion points.

- **Implement good loss prevention techniques.** For example, just-in time tenure review training for tenure committees or sexual harassment prevention policies can not only help prevent claims, but may be able to help mitigate losses when it becomes clear that individual employees responsible for the loss went rogue, and failed to follow the institution's policies, practices and training. Training is the means by which we implement policies, so if there are specific policies in place that are intended to prevent losses, it is essential that training be provided and that it be documented. This will be a challenge as institutional leaders regularly comment that they are already under excessive demands on employees' time to participate in training. Risk managers need an effective method to provide and document that communication has been provided on policies and institutional expectations.

Taking these steps and integrating them into your risk management process will help your institution avoid claims and successfully manage them if they happen.

IV. Unique Elements by Type of Claim — During the Loss (or Keeping a Medium-Sized Loss From Growing Into a Catastrophe)

The participants worked with three case studies for claims over the course of the think tank. Recognizing that complex claims can happen in a number of areas, we looked at a hypothetical claim constructed from events drawn from the news media on property, cyber and mixed liability. The hypothetical claims have been edited in the interest of brevity for this publication.

Our objectives are to identify both the practicalities of managing specific types of complex claims as well as the unknown or unexpected issues that can arise in these matters. For more information on property losses from natural catastrophes, see the Gallagher Higher Education Think Tank Study: Natural Catastrophes on Campus, 2011.[1]

A. Property Claims

Certain types of property claims are likely to be complex. These include property losses that involve multiple facilities; certain types of locations (such as libraries, research centers, sensitive equipment requiring careful calibration or animal research); or certain causes of loss, such as earthquake, hurricane or flood. Pollution resulting from an insured event is nearly always a complicating factor. Business interruption (BI) and/or contingent BI (such as loss of significant vendor or supplier, or closure of transportation to/from major campus) will often complicate an otherwise straightforward property loss. The involvement of FEMA or its state equivalent will add to what is already very likely a complex claim. We crafted a hypothetical situation from a number of these elements.

Hypothetical Situation

An intense summer wind and rainstorm knocks out power on a campus for 36 hours and causes significant property damage to the institution's science center, a three-building complex that includes classrooms, faculty research labs, the animal research center, a greenhouse and a campus café. The storm happens on a Saturday, two weeks before the last of the summer programs are over and three and a half weeks before the students arrive for the start of the semester. A STEM summer program sponsored by the institution is supposed to begin the following Monday.

- *Some of the animals are lost due to flooding. At least one of the animal studies has been ongoing for more than 20 years and involves genetic transmutation. At different times the value of the animals has been estimated at $14 million, $7 million and $1.5 million.*
- *Other research losses include frozen tissue specimens gathered over 20 years for study in a specific research project. The research samples are extremely difficult to put a value on.*
- *Property losses include damages to a specialized building, highly specialized and expensive equipment, plants in the greenhouse, and personal property of faculty.*

A few weeks following the return of students and faculty to the building (mid-September), there are multiple complaints of intense headaches, rashes and other symptoms typical of allergies, but EH&S tests do not indicate any cause. Complainants say there must be mold and other storm contaminants in the HVAC system.

Claims Issues

- Property damage to the building, contents including scientific equipment and the lost animals
- Potential BI/extra expense claim (café and summer program)
- Expenses of replacing animals
- Valuation of lost research
- Possible loss of grant funding
- Disruption of the summer program
- Property damage identification and clean up
- Other extra expenses (employee time for cleanup; will programs have to be displaced? How will the summer program be handled?)
- Cost of testing for contamination
- Cost of possible mold cleanup
- Communications costs

Coverage Issues

- Wind coverage: Some insurers may restrict coverage for windstorms or named storms, including having higher deductibles on the storms.
- Flood coverage: How does the property policy cover flood damage?
- Extra expense coverage: Are there adequate sublimits to cover the losses?
- Business interruption: Are there any time limits that would impact the coverage?
- First-party pollution coverage: Will the policy cover the detection and removal of mold or other contaminants?
- Increased cost of construction: Are there adequate sublimits to cover the losses?
- What documentation is needed for recovery?
- General liability and workers' compensation policies may also be triggered by this hypothetical with respect to the alleged building contamination.

Research institutions may have unique business income risks related to the high percentage of international students in their school. If the research is lost or stalled, enrolled students may choose to leave and pursue studies elsewhere. Depending on the length of the interruption involved, new students may not enroll, causing a drop in enrollment over multiple years.

Complexities

In addition to the general issues that can create a complex claim, property losses have some unique issues that can prove challenging.

- If this was a regional event, all business owners will be scrambling for contractors, labor and materials to bring their facilities back into operation. If any of the buildings were very old, the institution may have to bring them up to code and possibly have to consider historic preservation requirements. It is critical to understand how to access the increased cost of construction coverage in the property insurance and adequately document the expenses to ensure coverage.
- The research lost in this storm event is considered to be a complexity for the claim. The claims response team will want to help the researcher develop physical evidence of the value of the lost research (animals, tissue) as accurately as possible in order to make a claim that will not be contested. Documentation is essential; the objective is to gather sufficient evidence to be able to quantitatively value the property. This can include identifying original costs, time and resources put into gathering or creating the physical property, or possibly an opportunity to purchase similar property from other sources (parallel research in another region of the country).
- The nature of the contents of the building may present unique risks. While cafeteria furnishings and food handling equipment is readily available, some lab equipment may have long lead times to obtain unless the institution is willing to purchase refurbished used equipment. Faculty may object to the used equipment. The classroom furnishing may present an issue of lead time. Depending on the policy terms, the research animals may or may not be insured.
- Who owns the contents adds another complexity. Are students, faculty and staff aware of their and the institution's respective obligations if their property is damaged? Depending on the policy, personal property of others that is lost in the event may or may not be covered by the institution's insurance. Managing personal property claims in addition to the institution's claims can greatly complicate the claims management process.
- Loss of power creates a cascade of issues and claims. Part of the emergency planning process should include the identification of critical facilities and the costs that would arise if the facilities were without power for an extended period of time. In some zones, the loss of air conditioning would be critical to the facility's function. However, with regional issues, if the generators are not run on natural gas, there may be shortages of gasoline or diesel fuel to run the generators, and few people to get the fuel and bring it to the generators. Consider these issues when adding generators to a facility.
- Complexity of the claim is increased exponentially when the loss involves BI, especially for medical facilities. This is one area where external help is essential, such as a forensic accounting firm to determine the loss and keep track of costs.
- Does the institution lease sections of the building to third-party tenants? Are copies of those leases available? They should identify the institution's and lessee's responsibilities in the event of a loss. Copies of all leases will also need to be provided to the carrier.
- If the institution leases the space, the same considerations apply. The institution will need the lease agreements and an understanding with the lessor about mitigation, repairs, access to the space and possible lease termination provisions.

- What insurance policies might respond? Just as multiple claimants may be a coverage issue, multiple insurance policies also complicate the management of the claim. Tracking costs and allocating them to the appropriate insurer and making sure that the provisions of each different policy are being followed can be difficult. If there are overlaps in coverage, the institution may be caught in the middle of two insurers, each looking to be the second payer. Being hit with multiple deductibles or retentions can really affect the bottom line. Make sure you engage your broker right away to make sure that all of the institution's claims are reported and that reporting thresholds are met. Always check the policy for endorsed coverage terms.

Before the Loss

As with many risk management issues, when it comes to complex losses, pre-planning will save the institution time and money. Here are suggestions specific to property losses on what to do before the complex claim hits.

Know the Risk

- Develop your SWAT team—consider including director-level positions for Finance, Dean/Provost, Facilities, Information Technology, General Counsel, EH&S, Risk Management, Human Resources, Campus Police and Emergency Response. Include these individuals in any loss drills.
- Get researchers and facilities with high-value equipment to complete valuation schedules. One of the key issues that can make a claim more complex than it has to be is uncertainty regarding values, and lack of documentation that could help establish existence of equipment and its value. See the appendix for a sample worksheet. Know that the school could lose grant funding if there is a loss of materials, and determine if this can be included in the BI claim (best practice is to value it in the BI income statement).
- Do complete a BI worksheet. This is often seen as a total nuisance by risk managers, but having it done in advance can provide a road map on addressing the BI losses.
- Understand the impact of a long closure on students. Sometimes other revenue resources will be impacted if the campus is closed. For example, the VA may give scholarship funding to veterans that is conditional on the school being open (i.e., the students enrolled) by a specific date. If the school is closed due to a serious loss, those students may lose their funding. Other students may be graduating and have jobs lined up. For these reasons, having adequate extra expense coverage and a response plan in place is essential.

On forensic accountants:

We sit down with the forensic accountants early on in the loss management process so that we know exactly what we have insured and it is well organized on a spreadsheet. We give them the entire property schedule so they know what's on there. They also know what every deductible and sublimit is per type of loss or coverage. We also have them loop in mitigation or restoration service providers. This allows us to tie in to what FEMA wants to see. So that really becomes the crux of your claim paperwork, if you will. Because if that piece doesn't work, you're dead in the water—all this information has to be put into what you provide your forensic accountant.

Have Your Response Teams in Place

- Make sure that you have contracts with restoration companies so that you can ensure that they will come to your institution first, in case of a regional event. Pricing should also be set in the agreements so that you are not subject to price fluctuations because of resource scarcity. Another concern is that you might have a claim covered by FEMA, who requires that the institution goes out to bid before hiring. If you had to do that at the time of the loss, it could take 90 to 120 days. Be sure to keep your bidding and selection documentation in support of your FEMA claim.
- As important as restoration services are to physical recovery, forensic accountants are vital to financial recovery. Have a retainer contract with a company so that they can provide support on the loss cost analysis and tracking. Smaller institutions may simply use the firms recommended or required by their insurer.
- Set up your mutual aid agreements in advance. Sometimes, even informal agreements can be helpful. For example, if a school needed to temporarily store items at an off-campus site, having such an arrangement could be important. These types of arrangements can also help the institution relocate researchers to other schools while their lab is being restored.
- Have a good relationship with your municipal police and other offices—you may need to have a police presence on campus, as well as support on permitting and other regulated activities. In some instances, schools have used state police and even national guard in the aftermath of severe hurricanes. Knowing how you will obtain and coordinate services can potentially save the institution a significant amount, reduce potential additional losses and eliminate increased complexity of the existing loss. A forgotten aspect is that the municipality may have built the institution's campus and resources into their emergency response plan; they may expect to be able to use the institution's gym or campus center as shelters, and the institution's parking lots for vehicle staging and management. Know and prepare for what services and resources your institution will give to the community.
- Identify essential institution personnel who will be needed to maintain campus operations in a loss.
- Have a system in place to track documents and costs related to the loss. This includes items such as pictures of damaged areas, vendor estimates, an invoice tracker, etc. Consider setting up a new accounting code for a specific loss and its related expenses. This will add value to the process in automated reporting. Periodically share the cost information with your claims adjuster so they have real-time information about how the claim is progressing.

Communication Strategies

- In a serious regional catastrophe, like a hurricane, with long power and cellphone disruptions, institutions have found success in going back to old technologies. One institution had a radio station with a crank generator and was able to use it to broadcast information about school closings and openings, where to go for resources, and other assistance and recovery news.
- Campus ham radios have also been wonderfully helpful in communicating in the midst of a crisis.
- Hard-wired phones, another "old" technology, may be running even if cell towers are down.
- Using a pop-up or emergency website hosted at a remote location was a commonly mentioned strategy to keep people informed at many participants' institutions. Very large institutions will want to select a host provider that can handle a lot of traffic because an overload can create denial-of-service problems.
- Social media will be available if cell service is up. Sometimes this can be the only way to communicate by cellphone. Keep in mind that all updates on social media and the internet should be managed by the communications team for consistency and appropriateness of messaging.
- Google Hangouts can be a good way for members of a team to communicate as a group, with all members being able to post and see messages for the group.
- Consider using Government Emergency Telecommunications Service (GETS) cards.[2] GETS is a program of the Department of Homeland Security, Office of Emergency Communications that prioritizes calls over wireline networks. Users receive an access card (GETS card), which has both the universal GETS access number and a personal identification number (PIN). To get priority access over cellular communications networks, you need to use the Wireless Priority Service (WPS) program. GETS and WPS can be used in combination. The GETS program is in effect all the time—it is not contingent on a major disaster or attack taking place.
- Don't overlook local county or city emergency teams in the communications process. Know who is responsible to take the lead so that people are not talking over each other. Stick with the emergency response plan.

Risk Management Responsibilities

- Set expectations with leadership as to what is and isn't covered as early into the claim as possible so that reserves can be set and funding appropriated for uninsured losses.
- Ensure that leadership assesses whether or not the institution can reopen, and how quickly it might happen. Some disasters, e.g., Katrina, can result in a complete closure for a semester or more.
- Remind and outline the loss documentation and tracking process for all recovery personnel.
  - » Snap photos of damages on your cellphone before removing or fixing.
  - » Use the system for all work orders and invoices, storing photos, and identifying damaged property and equipment.
  - » Contact the adjuster for a visit prior to disposal of designated equipment or items.

Role of the president

Help senior leadership, especially the president, understand their role in a crisis as soon as they come to the institution. Tell them, "We need you to do the following [defined role and responsibility] and be ready for the phone. We don't need you at the table managing the details." When presidents get too deep into the weeds it just disrupts the whole [ERM] planning process that the school has worked on for years. So I think this is something we all need to do. Our readers need to know that they've got to have that conversation with senior leadership and incoming presidents.

[2] https://www.fcc.gov/general/government-emergency-telecommunications-service

An institution began building a new mixed-use student residence hall for its inner-city campus. The cladding for the building was sole-sourced from Canada. The manufacturing plant burned to the ground and the loss of the cladding impacted the construction dependency sequence, causing an estimated two-month delay to the opening of the residence hall. The institute incurred expedited costs to re-sequence construction to remove cladding from critical path. However, the insurance policy had a $1 million limit on materials stored internationally, leaving the school with a multimillion-dollar uninsured loss. Risk management was unaware of both the sublimit and the exposure.

- Make sure that all policies with a potential for coverage are put on notice. If you have a water loss, inform your pollution liability and cleanup coverage carrier even if you are still unsure that there might be a claim.
- Talk with your finance department about their cash flow needs and advise when recoveries (i.e., payments from underwriters) will be made. Be sure to work with the broker and insurer on securing advance payments to enable quick payment of recovery expenses to help ensure that cash-flow needs are met.
- If working with a disaster response and mitigation company, check with both the company and the insurer on payment scheduling; some mitigation companies may be willing to reduce their overall charges if they are receiving payment directly from the insurer.
- Pull out the BI worksheet and share it with your accounting team to ensure that they have the roadmap for recovery
- Use crisis communications insurance coverage, if available, to obtain professional support for the institution's crisis communications plan.
- Try to get a rough estimate on the size of the loss. This can be very helpful in avoiding the cycle of adjusters, so that a large loss adjuster is assigned at the start of the claim. (Many insurers will assign less experienced adjusters to claims up to a certain dollar-loss threshold, with more experienced adjusters assigned as the size of the loss increases). If this is the case with your insurer (you can find out from your broker), identifying the size of the loss early on can help avoid delays on claims processing due to changing personnel.
- Use the rough estimate information to secure an advance on the claim. These funds can be used to help offset immediate expenses regardless of what they are—for example, bringing in trailers to create temporary classrooms; work with the forensic accountants on tracking.

Other Situations to Consider

- The loss may not always be on the home campus. Consider how the institution will respond to significant losses in other locations where staff may be limited primarily to faculty and a couple of administrators.
- International losses (e.g., a researcher working abroad with extensive university-provided equipment or a sponsored study-abroad program overseas) may not be large in cost but may be extremely complex to manage. One participant described a 10-year research project in an African country that employed local staff, and had rented space, equipment and vehicles.
- Always check with the insurers when multiple events over a short period result in collective damages in order to mitigate the challenges of multiple deductibles or retentions. A few years ago Boston experienced a wave of major snowstorms—one or two a week for four weeks. Some property underwriters covered damages from these storms as one event.
- Many institutions will not have the necessary number of people in-house, or the right expertise, to manage and respond to a complex or large property loss. These institutions should be cognizant of this fact, and not try to do it all themselves. It will cost time and money.
- Contingent BI is becoming a bigger issue, particularly for metropolitan areas. While the institution may itself be relatively unharmed, infrastructure such as metro systems or access roads may be unavailable, whether due to catastrophic weather or terrorist attack.

- Contingent BI coverage may also be needed in a Builders Risk claim, especially if there are critical sole-sourced materials that go into the project. Check all large projects for sole-sourced materials, including their value and where they are sourced from to ensure that policy sublimits are adequate.
- Unintended consequences of mitigation actions must be considered. In one instance, in response to a school shooting, local regulators required that automatic locks be put on all doors in a building used to support allied health. Following a hurricane, the loss of electricity meant that the doors could not be unlocked and, as the building flooded, the locked rooms became fishbowls. Only after electricity was restored could the water be drained from the building, a situation that exacerbated the loss.
- All large losses are negotiated. The importance of this fact cannot be understated. The better the institution's documentation is, the more likely that you will recover more of your losses.

B. Cyber Claims—Property and Liability

While the successful management of complex property claims involves preparation and practice, managing complex cyber claims points to advance work in communication and training, both in terms of understanding and explaining the coverage to key administrators and around loss prevention.

Hypothetical Claim

The FBI knocks on the door of a middle-level manager in IT and tells them that they believe a certain foreign government's defense units may be in the College of Engineering's computer system in an unauthorized way. However, they ask that no changes be made right away, because they are tracking their electronic movement, and to keep this confidential, explicitly prohibiting reporting the situation to management. Once they allow the institution to make corrections, it is discovered that:

- *There was a lot of old personally identifiable information (PII) on some of the computers.*
- *The intrusion was so pervasive that those computers and servers cannot be restored, and they must be scrapped. Data is also corrupted, requiring some research to be redone.*
- *They may have accessed some U.S. Department of Defense research.*
- *Other researchers were doing work for private corporations and there may be a data breach of trade secrets/intellectual property (IP) that may have been under a licensing agreement, and therefore to the benefit of a third party*

While this scenario may seem far-fetched to some schools, a number of participants volunteered that similar situations had arisen at their institutions. Some cases involved the FBI and others involved other federal agencies, such as the IRS. Targets included medical centers and their records, engineering research, plant/biological research, survey information, industrial labor relations, and weapons research (DoD). Multi-campus institutions or systems are often uniquely vulnerable, because a vulnerability exposed on one campus or in one electronic data system may be quickly attacked on other campuses.

Claims Issues

- Forensic investigation, notification and services to all owners of PII in the system—who is responsible for providing it? Variations include the insurer, a preselected consultant or the institution.
- FERPA notifications to student owners of personal information (e.g., grades, course evaluations) in the system—who is responsible for the notifications?
- Loss of research data—was any backup available?
- Loss of hardware—the hypothetical loss was worsened by the FBI's insistence on delayed response.
- BI (including additional costs incurred due to the delay requested by the FBI).
- Forensic investigation into potential compliance breaches.
- Notifications to DoD, other federal agencies on particulars of breach and contract issues.
- Potential loss of grants (government versus private sources and impact on grant funding).
- If private research was compromised, does the private licensing party have a claim against the university for loss of market value, etc., if their licensed IP was jeopardized?

Coverage Issues

- What coverage is available under the cyber liability policy for any of these costs and expenses?
  - When reviewing cyber policy language, look for consequential reputational harm; this provides coverage for lost profits because of reputational damage resulting from a covered event. Coverage will define a reputational harm window, which is a period of time following the discovery of the cyber event.
- Is any coverage available in addition to the cyber insurance policy? Possibilities include:
  - Property (damage to hardware, network infrastructure)
  - Crime (theft of assets via a cyberattack)
  - K&R (ransomware attack)
  - Crisis communications (reporting to the community about the loss, managing media reports)

If so, how do the policies apportion coverage, or are the coverages separate?

- Increased costs caused by delays imposed by governmental authority.
- What insurance limits apply and how adequate are they? This hypothetical loss might cost $10 million or more; most schools' cyber polices have less than $5 million limits. See the Gallagher Higher Education Liability Benchmark Report 2018 for more information on insurance limits.[3]

Complexities Specific to the Hypothetical Loss

- The delay in notice imposed by a federal authority can go all the way up the reporting, or escalation, chain: the CISO and CIO receive late notice; the RM receives even later notice; insurers receive very late notice. This may compromise coverage and the ability to respond to minimize or mitigate losses.
- Most states require "timely notice" to individuals whose records have been improperly accessed. Multiple states' requirements are usually best managed by a firm specializing in such notification; insurers may even specify the firms the insured must use. If medical records are involved, state law may require patient notice within statutory time frames even when there is a criminal or other investigation into whether or not the unauthorized access actually occurred.
- Systems need to be secure before you give notice, because the minute notice is given, hackers know the system has been compromised and will redouble their attacks.
- Plus, internal obstacles may complicate the loss:
  - Cross-unit priorities may differ (IT security vs. IT operations vs. research vs. legal vs. compliance vs. government relations vs. strategic/media communications vs. risk/insurance management vs.…)
  - "Who is going to pay for all of this?"—Departments may end up squabbling over limited insurance dollars; recovery may be hampered by a lack of funds.

Before the Loss

A clear understanding of the cyber risk landscape will be tremendously helpful in managing cyber losses. Understanding policy terms and conditions will help to match the losses to the appropriate coverage, and select coverage terms to meet institutional needs.

As mentioned in the previous section on claim preparedness, develop your SWAT team—consider including director-level positions for Finance, Facilities, Information Technology, General Counsel, Risk Management, Campus Police and Emergency Response, and include these individuals in any loss drills.

Valuation of equipment and data

Knowing the values at risk is important in correctly choosing insurance values.

- Particularly with research data, the concerns may be not only that someone saw or downloaded the data, but that someone corrupted or changed it. If there are concerns that the data can no longer be trusted, it may be prudent to have the integrity of the data assessed. The cost of such an assessment would have to be weighed against the value of the research or the cost to duplicate the research.
- Hardware is typically covered in the property policy, but risk managers should ensure that there is coverage for hardware corruption caused electronically by criminal or other acts, such as malware introduced by a phishing attack or removable media. Also keep in mind that replacement coverage is for like kind and quality. In this fast-moving environment of tech, IT teams and researchers will not usually be willing to replace damaged equipment with equipment of like kind and quality—they will want to replace it with the latest and greatest. For computer hardware, check with your broker to determine if the policy can be endorsed to cover purchase or replacement cost, whichever is greater.

[3] https://www.ajg.com/us/-/media/files/us/insights/market-reports/gallagher_higheredliabilitybenchmarkreport_2018.pdf

- Understanding the BI loss is necessary, both in amount and cause. Policy clauses may or may not cover BI caused by federally mandated delays—e.g., the institution has their hands tied because they had to wait for the FBI. One school settled on the overtime of personnel involved in their forensic assessment but did not recover any expediting expenses. Does the policy even cover BI? Are there limitations on the trigger (e.g., system failure, programming error, or cyberattack)?
- Contingent BI is another consideration. What if the loss is in the hands of a third-party IT vendor or a cloud storage service vendor? How do the vendor contracts protect the institution (or not)?
- Exposure of PII is traditionally based on the number of records—does the institution know how many records are at risk?

Where are the problems and added risk?

Cyber risks are complex in and of themselves aside from the claims. Risk managers need to identify where there may be risks on campus as they assess how to address them.

- Departments that may be running their own systems and servers are more likely to be vulnerable than those falling under the jurisdiction of a centralized system with high-level security controls in place.
- Alumni associations may have a lot of PII records and may operate their own systems. Are they insured? Is it a separate legal entity, or staffed and managed by the institution? Even if the organization is a separate entity, there may be reputational risk to the institution; how will that be addressed?
- University business incubators may be another source of risk, as they may be housed off-site, with their own systems, and whose data may be particularly sensitive. If the "next Facebook's" startup information is stolen or compromised, who is liable and for what?
- Other affiliates, including health clinics, need to be covered either under the institution's own coverage or separately.
- Does the institution have the care, custody and control of other people's data such as PHI, or other people's data on research? Is it stored in institution-owned or on third-party servers (cloud)?
- Are there any areas where the institution is a vendor for computer services for others? For example, an institution is developing software for sale. Hopefully the contracts go through counsel who can alert risk management to the exposure.
- Contracts and their clauses may create particular types of cyber risk; institutions can manage these risks through a thoughtful contracting process. For example:
  - » Cyber requirements in sponsored research agreements may create privacy and security liability for the institution. It is important that the institution assume responsibility for its operations only.
  - » Vendor or contractor contracts may seek to limit damages to a service fee or low dollar amount, so negotiate any damage limitations to be not less than required insurance limits.
  - » Vendor or contractor services may create potential privacy and security exposures, so the institution's contracts should require that the contractor carry cyber insurance with reasonable limits.
  - » Institutions can contractually require that the vendor must meet industry and regulatory standards, and accept liability for failure to meet or operate to standards.
  - » A contract vetting process that uses IT and risk management expertise provided by the insurance carrier and insurance broker can help to manage transferable cyber risks.
  - » Sometimes, contracts are not as negotiable as one would like. Tell decision-makers what the impact could be when contract terms are unfavorable
- Some institutions are joining forces to work on issues like third-party/vendor screening or creating a base security center. The institutions are relying on each other to protect data and make decisions, for example, on approved software or vendors. These programs should be insured and have clear ownership and liability delineations through contracts, as well as protocols for when one institution rejects the findings of the group or association.

The perils of providing notice of a breach:

We provided notice after we were given that guidance by legal counsel, but then we were told by the FBI, "You need to shore up your systems because the minute you give notice, the minute you say that you have been hacked, you are telling the hacking community that you're hackable. And then you are going to get many more hits." Yes. And so, that indeed happened. The Friday that we said we have been hacked, we were hit like 700 million more times. And we had to be prepared for that, we had to have the system and the support to be prepared for that, which we would not have otherwise known at that time.

Risk and Recovery: Coverage Comprehension

It is the risk manager's responsibility to know what coverage is available and how it applies. The institution's insurance broker can provide assistance in this as well.

- Check your insurance policy—there's language in the insurance market that allows you to delay notice if there's an active criminal investigation going on that prevents notice to the insurer. While it is not automatically provided on all policies, most carriers will accept that type of language if requested.
- Institutions may want to negotiate an annual deductible cap in case they have a series of breaches or incidents.
- It's also important to carefully craft the notice pool or reporting officers, i.e., the individuals whose knowledge of an event triggers the notice requirement to underwriters for coverage. This has to be crafted so that it makes sense within your institution's escalation process, and so that it will get to your risk manager and chief information security officer.
- Work with your broker to do a coordination of coverage and gap analysis across the entire insurance portfolio. This is very important, as coverages and recognizable exposures are continually changing. For example, how is biometric data gathered, stored and used at the institution? How is the institution protected against misuse?
- Work with your insurance broker to understand what policies other than your cyber policy may apply to a loss. For example, if there is physical damage to hardware, electronic data, programs or software, the property insurance may apply. If the institution is subject to a ransom demand, the cyber policy may cover it or it may be covered by a special crime (K&R) policy. A forensics investigation into the ransom demand may be covered by all three policies. Work with insurers in advance to have other insurance clauses that will protect the institution.
- Develop a defined escalation (communication) process within the institution on the notification of incidents, breaches or other IT losses. Define who receives notice, when they receive notice and for what types of incidents. It is better to be over-broad than too narrow in scope.
- Know what specifically triggers notice; some coverage may state that the notice trigger or period begins once you've completed an investigation so that you can determine that you actually have had personal identifiable information compromised.
- Carriers are also improving insurance steadily. For example, one carrier is offering coverage for betterment costs to improve systems. Keep in touch with your broker for updates and add new coverages to your policies by endorsement.

Risk and Recovery: Coverage Communications

- Know your state laws with respect to notice requirements.
- Contract with a firm such as Experian to offer credit monitoring services to employees or third parties who may have had their PII breached or as directed by the insurer.
- Work with the IT department on notification of incidents. Develop an appropriate means of communication with insurers to put them on notice of a possible loss and criminal investigation without compromising confidentiality.
- Create a timetable for notice on PII and other required notifications so that everyone on the team understands the institution's compliance obligations.
- The institution should complete and regularly review its data classification, i.e., organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve, and can also help an institution create a data security plan that accounts for differing levels of data security based on data sensitivity. This is particularly important for risk management, legal discovery and compliance.
- Related to the data classification program, IT should know what departments or operations are hooked up to the university system that are running their own servers and software, and ensure that all such operations are fully compliant with all security protocols.
- Consider creating a cyber governance committee with faculty and academic advisors to help be part of the solution of cybersecurity and faster incident response. At one institution, this committee meets quarterly and is attended by a presidentially appointed cyber risk governance executive from each campus, who has direct contact with the chancellor of the campus. They keep their meetings fresh and relevant by reviewing actual situations, breaches or near misses.
- Proactively educate staff about the institution's cyber coverage. Schedule a meeting with the underwriter and possibly their response team to walk the IT, GC and RM teams through the coverage, what is covered, reporting a claim and managing the loss. They can be brought in to do workshops on a specific regulation or event, like a ransomware attack or network outage. Make full use of your underwriters. This can be especially important if the insurer requires preselected forensic response teams, attorneys or other service providers in the event of a loss, so that responding departments know that they cannot simply hire the service providers they like. Do this whenever the institution experiences a significant turnover of staff or a new insurer.
- If your insurer will accept alternates to their preselected panel of service providers, negotiate the firms the institution would like to use in advance of a claim. Pre-identify the forensic and legal partners, and manage the conversation with RM, GC and IT. The board may think the best people are in expensive metropolitan firms, but local resources or resources elsewhere in the U.S. may be as good or better, as well as less expensive. It's always best to have proactive communication with the broker and insurer. An argument on the economics of using particular counsel (e.g., cost/hour, efficiencies, etc.) can help manage expectations with both underwriters and boards.
- Cyber risks should be one of the tabletop exercises that is included as part of the institution's annual crisis response preparation. Bring in experts from the outside to help with the planning and execution. Consider different approaches, such as a focus on a specific threat or focus from a legal, governance or compliance perspective, or a deep dive into a technical response. Using a variety of approaches can keep the drills fresh and innovative while helping to ensure that everyone is on the same page after a loss.

Avoiding the Loss—User Education and Training

- Mandatory online awareness training of all system users (faculty, staff, students and contractors) on issues like passwords, system security, phishing and other attacks is very effective in reducing claims arising from users. Consider using the carrot or the stick approach (perhaps in combination). The threat of removing access to the system (with notice, of course) ensures 100% compliance with training requirements. For new users or new systems/software, the institution can require passing a training to gain access to these resources.
- Assess what is on your website that is facing the public and ask if it needs to be there. Strictly administrative procedures—like instructions for employees on how to change their bank information—should be behind a firewall.
- Provide training. Perfect is the enemy of good. Just because certain off-the-shelf products are generic doesn't mean that they are not effective. Schools that do not provide training because they insist on using only custom products may lose out, not only on any benefit that the training itself might provide, but also as a defense against negligence or noncompliance. Some institutions purchase off-the-shelf training and later develop training that is institution-specific while other schools simply rely on off-the-shelf training.
- Positive results are accomplished when the focus was teaching people that they are the protector of the information. This makes it less of an IT problem and more of an understandable people problem.

Know your CIO and CISO

No matter whether you're big or small, the risk manager needs to become a friend to their chief of IT or IT security officer. Let them know risk management's role in evaluating and identifying risks. Let them know you've got the insurance coverage in your back pocket. They need to know you as much as you need to know them.

- Some schools use targeted training like fake phishing. If the user falls for it, the system sends the user back for retraining.
- Ask your IT team to keep statistics or metrics on accidents, such as accepted phishing attacks or other user-related incidents, and chart them against training to assess effectiveness of current training.
- Note that insurers may provide complementary services or even grant money for phishing training.
- Central administration can help tie compliance to results by offsetting insurance retentions if the responsible department is in compliance; if not, require the department to pay some or all of the retention (incentive program). Departments must be informed and reminded of this policy.
- Don't overlook your records retention and destruction policy. Removing old records when legally appropriate can greatly reduce exposures. Include training on records destruction in the training materials, and encourage employees to appropriately discard old records.

Critical Steps Following an Incident (Breach)

- Inform your insurer/s and broker with as much detail as possible about the incident. Do not delay on this action. Follow policy requirements on incident response to ensure that coverage will be applicable.
- When the institution has an incident, a forensic analysis must be done as quickly as possible to determine if there has been any breach—it is usually necessary and best practice to bring in someone from outside. The service provider may be specifically assigned by the insurer, the institution may choose from a select pool of providers, or the school may be able to select their preferred provider with underwriter approval. As noted above, it is always best to know in advance who will be used.
- Once a breach has been confirmed, additional investigation needs to be done to determine whether data was accessed and, if so, which data and whether it was exfiltrated. Outside counsel may be needed to evaluate whether a breach triggers issues with the OCR or certain state agencies.
- If the institution is part of a system, all other institutions should be investigated as soon as possible for similar breaches, since they all likely use the same security structure.
- If data has been exfiltrated, and if the institution will be handling the notifications, create a chart on the mandatory timing of notices to help with notice compliance. If using an attorney to provide notice, ensure through the contract that they will be responsible for timely notifications.
- Engage with the communications team and, if appropriate, the institution's crisis communications consultant to carefully craft notice to the affected community and its timing if the breach is very large or if PII or PHI was compromised.
- Identify all other possible claims that might arise from the incident or breach and notify other insurers as may be applicable.

Other Situations | Post Claim

- Schools that have had large claims report that IT is more receptive to working with risk management on best practices and underwriter recommendations, as well as reporting to underwriters what the exposures are, completing the underwriting questionnaires, etc.
- Use the departure of a CIO to revisit and refresh the IT systems at the institution. While the decentralized approach works well for most higher education operations, it is antithetical to computing security, data management and incident response. Implement multipart securitization. Centralize these operations as much as possible, building in performance metrics on security, employee training and compliance.
- Some insurance policies require that a preselected breach coach be used to access coverage. This is done because the underwriter wants to minimize the possibility that the insured will make any errors in their breach response, thus potentially complicating the claim. This approach is not always welcomed by the general counsel's office or IT, sometimes because these offices doubt the breach coach's expertise or their ability to work effectively within the institution. This may be a consideration in selecting insurers, or it may simply mean that additional work, through introductions, workshops or other intervention must be taken to ensure that the process is correctly followed. Reminding the recalcitrant administrators that the process must be followed in order to access insurance funding is sometimes the last option.
- If high-profile donors or other VIPs need to be informed about a potential breach, consider having a process to gently inform them in advance of the issuance of the legal notification letters. Your crisis communications policy may help with this.
- Enforce your records retention and destruction program. Utilize bots or other automated systems to crawl through data and tag old data for destruction. Limit the data as it is transferred to a cloud or other storage facility—don't allow data that doesn't meet qualifications for long-term storage to be put into storage. Send it back to the sender and ask them to determine if there is a need to continue to retain the data, or if it should be properly deleted.
- Confirm and train users on the institution's policies for disposing of old electronic equipment. This includes everything from servers to memory sticks. Require encryption of all sensitive data on all equipment and prohibit transfer of sensitive data to personal equipment.

Summing Up

Cyber risks will continue to expand as institutions rely more heavily on technology for both academic and administrative functions. While computer technology has now been available for several decades, there is still a relative lack of experience among campus administrators in understanding and responding to a cyber breach, in contrast to property or traditional liability losses. Moreover, cyber breach insurance coverage is relatively new to the marketplace and to insureds. The issues are compounded with the increasing legal mandates, and the continued development of electronic technology.

C. Liability Losses

Complex liability losses can be very different from property and cyber losses. Their dollar value can be unpredictable and difficult to assess because it may be dependent on third parties, like juries, and the response can be very difficult to control. All the recommendations of the think tank participants pointed to a simple, but not necessarily easy, approach: proactive notice to the insurers and good communication with them throughout the claim management process; sound choice of counsel; a thorough internal investigation; good internal communication on the claim and its management process; and a thorough follow-up on root cause, effectiveness of management and future prevention post-claim.

There is an apparent inverse relationship between transparency (internally and with carriers) and a worsening claim situation. The longer an institution (or an individual employee) ignores, brushes aside or covers up situations that might lead to a claim, the more complex the claim is likely to become. However, schools have concerns that transparency on open investigations of alleged misconduct may result in additional claims being reported (#MeToo) and that the accused will have suffered significant harm if found to have been innocent of the allegations. Is there a way for an institution to be transparent about such matters, perhaps by a simple statement that "X is currently on paid leave while the institution investigates allegations of misconduct"? Institutions' leadership will likely have vigorous discussion on such matters, and the results will be a reflection of the institution's culture. But it is much better to have those discussions and reach resolution before an incident than to have to force a decision when an incident has become known and the clock is ticking.

Hypothetical Claim

An adjunct faculty member tries to report being sexually harassed by the department's star researcher to her department chair, but is brushed off before she can say much. The adjunct faculty member doesn't try to report to any other responsible office (Provost, HR or the Title IX Coordinator), but tells her adjunct colleagues instead. Her contract is not renewed at the end of the semester. The adjunct sues the institution, her department chair and the researcher for sexual harassment, sexual assault, retaliation and breach of contract a few weeks after she receives notice that her contract will not be renewed. She also takes to Twitter, Instagram and other social media and begins to publish her diary, as well as texts and emails between herself and the researcher. Several other adjuncts come forward with similar complaints about the researcher and another member of the department who allegedly gave them unwelcome attention. Complaints include unwanted touching, forcible kissing and groping. At the start of the semester, undergraduate and graduate students become aware of the situation, and several students come forward with similar reports against the professors. One student alleges that the researcher engaged in a "consensual" relationship with her while she was a 16-year-old first-year student and, when she wanted to break it off, he hounded her out of the department. Two other women who dropped out of the institution allege similar circumstances. Students and adjuncts allege a hostile environment pervades the department, discouraging women from majoring in its studies. A few allege serial harassment in exchange for grades and access to research. Though the school has been engaging counsel on the matter for months, the risk manager only hears about the matter when it makes national news.

All the women complainants eventually join forces to file a class-action claim against the previously named parties including the institution, the professors and the department chair, as well as adding the tenured members of the department, the president, the director of human resources and each of the trustees. Allegations include lack of information and training on sexual harassment prevention and reporting, lack of policies regarding student/faculty relationships, and lack of oversight. All allege that it was widely known across the institution that the department had this particular misogynistic climate.

The president suspends the faculty members without pay pending an investigation. The investigation proceeds very slowly, and eventually their dismissal is recommended. They are dismissed before the court cases are resolved, and they sue the institution for failure to follow process and reverse discrimination.

The state that the institution is in begins an investigation into one of the respondents and the institution over the sexual assault of minors. The trustees fire the president for the debacle, whereupon the president sues the institution over her severance and alleged breach of contract.

This hypothetical scenario is an amalgam of claims recently in the news. This type of circumstance is by no means unique, particularly in the current #MeToo climate, where one claim frequently mushrooms into multiple claims.

Claim Issues

- Multiple claims are involved—issues include multiple deductibles or retentions and possible need for separate defense counsel for named defendants.
- Multiple years involved—issues include multiple deductibles or retentions, changing terms and conditions.
- Multiple coverages (general liability, employment liability, educators legal liability/D&O, excess liability and excess educators legal liability) policies may be involved.
- Delayed reporting of the claim may result in denial of coverage.
- Failure to report sexual molestation allegations to proper authorities may negate coverage.

Complexities

- The incident starts as a report of sexual harassment and snowballs into a class-action suit. The development of the claims over time—the moving target—complicates the response and makes it more difficult to manage.
- There are multiple claimants. For the women complainants against the institution, their claim is simplified by their joining forces in a class-action suit. However, the school is still defending claims from the three faculty members and the president.
- There are multiple venues for the claim, including the institution's own investigation and response procedures, the legal system, and the Twitter-verse or social media. Reputational issues abound.
- This matter has all the earmarks of a complex determination of damages.
- State agency investigation into the molestation of a minor may complicate the investigation.
- Extensive discovery on all claims will be needed.

Before the Loss

As with our other claim types and other types of liability claims, proactively managing for the claim[4] before the loss was considered to be the most important risk management technique.

Develop your SWAT team. Consider including director-level positions for Human Resources, Title IX General Counsel, Communications, Risk Management and Campus Police, and include these individuals in any loss drills. Individuals such as the Provost, Dean of Students and the Athletics Director may also be included, as incidents may involve their departments.

[4] Some questions arose that were specific to Side-A D&O coverage, a stand-alone policy that protects the trustees. Should institutions purchase this coverage? Why or why not? What limits should be purchased, and what does it cost? Our research indicated that:

- Few if any public institutions purchase Side-A coverage.
- Large research or academic medical centers are the most frequent buyers of Side-A coverage.
- Institutions that have had severe D&O claims also tend to purchase Side-A coverage, if only to reassure their trustees. Most institutions buy no more than $10 million in limits.

We have not seen any Side-A claims paid for higher education institutions. It is possible that this coverage might respond if a claim were to be brought against directors and trustees if an institution is closed and the D&O or ELL coverage cannot respond.

Single-point reporting and escalation plan

Some institutions have one point of contact, one number (hotline) to make all reports of misconduct. The reports go to an individual or team who is responsible for ensuring that proper escalation, reporting and investigation practices are followed immediately. This creates a top-down management structure and is more effective than filtering the claim up through multiple offices or individuals, reducing the potential error risk. This approach also creates an effective audit point for compliance.

Communication/Escalation Plan

- All employees, students and other members of the school's community (volunteers, parents, contractors, guests) need to know where (or to whom) they can report incidents or complaints of misconduct, whether it is harassment, discrimination, bullying or other acts.
  - » All supervisors (including receiving offices like HR and Campus Police) need to know that they are required to forward all reports to a designated individual for assessment.
  - » Designated individuals may be responsible for action or to forward the report to someone who will take action (investigate and/or escalate further).
  - » Individuals responsible for investigation need to know who they have to contact to escalate the matter, including senior leadership, risk management and general counsel. Serious matters have to be escalated to the top of the organization—knowing what and when is essential.

A clear procedure of escalation and incident management is critical to preventing claims from mushrooming.

- In many institutions the reporting and even potentially the management of harassment and other similar claims are handled by different departments. Depending on whether the parties involved are faculty or staff, the reporting chain may go through the provost for faculty and Human Resources for staff. Inconsistencies in reporting processes, investigation and management of incidences is a primary contributing factor in turning serious claims into complex claims. It is essential that procedures be managed consistently, including moving a report up the escalation plan.
  - » Ensure that equity and fairness is considered and addressed in the internal claim management process, especially when the involved parties are from different constituencies (e.g., faculty/student; staff/volunteer).
- Escalation plans should include minor situations (e.g., car accidents) that involve key personnel (e.g., the institution's president, chancellor, provost or board member) because the position that the person holds will put the matter into the spotlight.
- Assess your escalation plans if your institution has recently gone through a very public claim or claims that created a lot of negative publicity for your institution. Also note there often is a spike in claim activity after experiencing a claim that attracts negative publicity and/or when a large verdict is awarded. Be aware new claimants may think they are entitled to similar or larger awards, be more willing to go to the press and less willing to work toward negotiated settlements.

- All insurance policies contain specific provisions governing the Insured's responsibility to report claims. With some exceptions for those with large self-insured retentions, most insureds have a duty to report written claims and demands for damages as soon as possible. Ensure your escalation plan includes informing the risk manager or equivalent when a written demand for damages is received.

- Similar to formal claims, insurance policies stipulate a duty to report incidents/occurrences that could give rise to a claim under the policy. This rather nebulous requirement is strengthened in general liability policies by a list of occurrences that require immediate notification regardless of the insured's perception of liability. Specialty higher education insurance carriers have expanded their list of occurrences that require immediate reporting. Some make sure all reporting officers are informed of these changes and their responsibilities to report these occurrences. Risk managers may choose to use a bordereau reporting system to report and track incidences that have been filed with insurance carriers. When using this claim reporting methodology, it is important to obtain agreement from your insurance carrier that this process will meet the reporting requirements stated in the policy.

- Claims made on insurance policies such as educators legal liability and employment practices liability have their own claim/incident reporting procedures that need to be carefully followed. Failure to report a claim when received or incident that could give rise to a claim when it becomes known to the insured can be grounds to exclude coverage. In fact, failure to report claims/incidences in a timely manner is the most commonly referenced grounds for excluding coverage. The sensitive nature of some ELL claims, particularly those involving high-profile people on campus, has been cited as one of the reasons for the failure to report claims in a timely manner. In years past, insurance brokers had some success in overcoming exclusions for late reporting, particularly when it could be shown that the insured did nothing to jeopardize the insurer's position. Insurance carriers are much less receptive to these arguments in today's environment. Establishing a consistent claim reporting and follow-up process is an essential step in maximizing coverage in your claims-made policies.

- If the reporting requirements are not clearly stipulated in the policy, a better practice than simply using the incident bordereau is to inform insurers when incidents become claims (written notice to hold the institution responsible for loss or damage), when claims become lawsuits, and when lawsuit defense reaches half the retention amount or as soon as the institution believes that the retention will be pierced. Do not neglect the excess carriers either. Keeping insurers informed will ensure that coverage is never denied for lack of notice.

> Concerns for confidentiality of a claim can complicate matters exponentially—more than one risk manager has found out about a claim only when they read about it in the national newspapers.

When the institution purchases a new type of insurance, bring stakeholders together to explain the coverage and what it means to the institution—"look what we have access to!"

Choice of Counsel

- If your institution has general counsel, build a strong relationship with the general counsel (and their team, if applicable). They are pivotal in risk management getting notice of claims, managing escalation of claims and selecting outside counsel.
- If a school doesn't have a general counsel, consider using a firm on retainer to act like a general counsel, or an attorney on call that selected administrators can call for guidance. Be mindful of potential costs with this model and have a plan in place to monitor billings.[5]
- If having control over choice of outside counsel is essential to the institution, it must be negotiated with the carrier in advance of the claim at the time the coverage is placed, or an insurer willing to cede that authority to the insured must be an ironclad factor in choosing your insurance carrier. Fighting this battle after the claim is made or choosing counsel not approved by the carrier may result in the insured having to absorb additional costs, ranging from the entire claim to a portion of defense costs in addition to the retention.
- Particularly for large institutions with locations across the state, or in multiple states, preselecting your panel counsel by line of coverage is an important step. In addition to their being approved by your insurers, make sure that they know the judges and prosecutors, as well as the local risk management team, the TPA, campus counsel and other partners in managing the losses.
- Be thoughtful about using china cabinet law firms—the firms that may not be local and that have the big reputation for matters where panel counsel may be more effective simply because they know the institution and how to provide a great defense at half the price (or less). Don't let opposing counsel's reputation necessarily scare you into using the high-priced firm. Engage your general counsel in having these discussions, and encourage risk management to have a say on counsel.
- Choose attorneys from law firms with proven track records.
- Electronic bill review processes can save costs.

[5] See https://www.acenet.edu/news-room/Documents/Managing-your-Campus-Legal-Needs-An-Essential-Guide-to-Selecting-Counsel.pdf

Governance, Training and Education

- Have clear policies on what constitutes wrongful conduct and how to report it. Identify mandatory reporters and make failure to report a disciplinary event.
- Have clear, consistent, mandatory training of all employees (faculty and staff) on:
  - » What is harassment and other prohibited conduct
  - » How to report it
  - » Document the training
  - » Repeat the training periodically
- Remind supervisors that no matter how annoying or contentious a colleague is perceived as being, they must listen to their complaints seriously and completely. Teach active listening so that they can (hopefully) get to the heart of the matter, determining how and when to send the report up the escalation chain.
- Documentation is necessary so that the institution has defense if an employee disregards the institution's policies and engages in harassment or fails to follow appropriate reporting procedures.
- Institutions need to be very careful to ensure consistency in policies, training and documentation across all departments. Training all supervisors and report receivers on the escalation plan will help ensure that claims are reported to insurers as well as to administrators who need to know.
- Be especially mindful of academic department chairs; they may rotate into the chairmanship every two to three years. They usually do not see themselves as supervisors or administrators, and need to be carefully oriented to their administrative responsibilities.
- Multi-campus institutions need to structure their escalation processes to include risk management and reporting to underwriters.
- Some underwriters have a list of incidents that must be reported whether they are a claim or not. These typically include a death on institutional property, any instance of molestation, sexual assault (which may or may not be defined), certain types of injury, etc. Be sure that all individuals in the escalation chain are aware of these requirements so that risk management will be aware of and have the ability to report these matters to underwriters in a timely manner.
- Be mindful of the employee turnover cycle and make sure that regular, repeated training is made available.

Crisis Management—Directed Services

- Not every liability claim will have a crisis management component, but some might. A kidnapping and ransom situation is one example. If the institution purchases K&R coverage, make sure that the process is known to and accepted by the crisis management and leadership teams so that services can be properly accessed. Deadly weapons assault insurance is a similar coverage that might have directed services. Risk management can engage with the response teams to identify the buckets of money and services that are available to respond to a situation.

During the Claim

Use the litigation management tools offered by the insurer, TPA or attorney—have a litigation plan in place before they get into the case in order to have a good estimate of costs.

Communications

- Ensure that there is a good flow of communication between risk management, in-house counsel and outside counsel so that everyone is kept up to date on the status of settlement talks or litigation, changes in allegations or charges, or new claimants.
- In-house counsel should communicate closely with both senior leadership as to the status of the claim and any new allegations or additional claimants. The chief communications officer should also be kept informed of changes so that any information about the claim that is leaked to the media is not news to them, so that they can get ahead of such leaks and control the message in the media.
- Risk management should communicate closely with the insurer on changes to ensure that the insurer is on board with the progress toward the claim resolution.
- The institution and risk management do not have to wait for the claim to be resolved before they begin to address organizational barriers, procedures or policies that led to the claim.

Investigations

- Schools are required under Title IX and other regulations to investigate instances of misconduct. Institutions can use in-house and outside investigators depending on circumstances including complexity of the incident, expertise of the investigator, availability of the investigator and fairness or appearance of fairness to the involved parties.

- The risk manager should always be aware of when claim investigations are ongoing, as should underwriters, even if no written claim has been received. This is to ensure timely reporting and coverage. Keep in mind, this may not be possible if the institution is served with subpoenas that have restrictive terms on them, i.e., they strictly prohibit notice to any person not served or specifically identified. Anonymous EEOC reports and investigations should be reported as incidents on the bordereaux.

- Keeping track of a broader scope of investigations may be impossible in large institutions, but the trigger of any investigation should be identified on the escalation chain for appropriate notification within the institution.

- Treat all complainants and respondents equally, regardless of rank or prestige in the institution. This is, of course, easier said than done, but deferring to rank and prestige is one of the major reasons that we have seen mushrooming claims. Important respondents are incorrectly assumed to be incapable of having committed the described behaviors simply because of their position. Similarly, complainants with no status may also be easily dismissed as being ignorant and lacking understanding of what happened. There can be no bias as to probability of action based on the status as a complaining or responding party.

- Make sure your internal investigators know what they are investigating. Usually the subject of the investigation is whether the respondent violated institutional policy, not whether or not they broke the law. This is true for internal and consulting investigators.

Other Situations | After the Claim

- Conduct a postmortem after the claim is resolved. Consider if there has been any kind of failure in the reporting, in the investigative process, in communications or what underlying causes may have created or contributed to the claim. Address these issues, whether through additional training, improvements in policies and procedures, or other steps. Were institutional policies followed throughout the investigation? How well was the claim managed? Was counsel effective?

- Sovereign immunity applicability and limits will vary by state. Make sure that your state institution takes full advantage of immunity statutes.

- Remember that claims can happen even when the institution and its employees did nothing wrong. The key is to not do anything wrong in the response process, either.

- Gina Smith, a leading attorney on Title IX matters, identified one of the biggest challenges in dealing with claims that occur over a long period of time. She calls it the "tyranny of temporal compression," which is so prevalent in social media. It refers to a situation that has evolved over months, even years, and when it gets to social media, all the events are compressed together, as if everything happened yesterday. There is not much that can be done about this except to have a good crisis communications plan and a clear message about the "when" of events, as well as the "who" and the "what."

- If the claim involves a high-profile person, make sure it is elevated right away, even if the underlying event is relatively minor. This idea has been repeated more than once in this paper because of its importance.

- Reputational losses can negatively impact the way that local courts—prosecutors and judges—view the institution, making it difficult to return to a pre-loss environment where the institution may have been given the benefit of the doubt.

- Some underwriters are expanding the definition of the reporting officer for sexual abuse, molestation and serial offenses. Risk managers and senior leadership will need to have a plan as to how these will be addressed in the institution's policy of claim reporting and escalation.

- Insurance companies are looking to reduce their claims complexities by including language to the effect that one perpetrator equals one claim. Risk managers must be kept updated on these changes and should inform leadership how such changes can increase the institution's exposures.

- Identify sacred cows—those parts of an institution's culture that are seemingly above the institution's policies and procedures. They are often just difficult topics—high-profile alumni, conflicts of interest or major sources of revenue, such as sports, programs that bring in large grants or have an opportunity to generate funds (such as ownership in startups). It is commonly very difficult for a risk manager to get traction on issues above their governance level, so it becomes incumbent on the risk manager to develop relationships that can lead to such concerns being heard and acted upon.

- If a claim is settled above a certain level, do a retrospective review and let the outside lawyer explain what (if anything) went wrong in the case and how it might have gone better. Such a review is best done within 90 days. Don't limit the review to just the case, but have counsel speak freely about what led to the claim: for example, was there a bad actor in the department or was it a cultural issue? If there are likely to be lingering issues, how can these be fixed? The claim review process should include a paragraph on what will prevent this from happening in the future. ERM processes may also address these types of issues. Smaller schools may bring the deans together for a postmortem—use it to create a training, learning moment.

Summing Up

Make sure senior management is aware not only the various types of coverages the institutions has purchased, but also the incident and claim reporting requirements.

V. Emerging Areas of Complex Claims

- Behavioral threats—are institutions being held to an unrealistic standard of having to identify individuals who may commit crimes? What is the liability of an institution that has missed the threat of someone who then becomes an active shooter?
- Respondent claims from students or faculty who were found to have violated institutional policies with respect to sexual misconduct are increasingly filing counterclaims against institutions for failure to follow policy (or due process for public institutions), defamation, lost opportunities and other damages. These can be exacerbated when local plaintiffs' counsel is a crusader in this field.
- AI/cyber-related claims may increase as algorithms are increasingly used in decision-making and other processes; we foresee claims alleging failures arising from their application (e.g., admissions discrimination) as well as losses driven by the malicious use of AI to destroy or disrupt institution property, data or systems.

- Privacy claims may be driven by conflicting state laws and international law, such as the EU's GDPR.
- The in loco parentis pendulum appears to be swinging back to an increase both in duty to students for personal safety and responsibility for student conduct even when that conduct would have been considered to be private, or not connected with the institution. Liability for student clubs and activity is on the rise.
- Athletic injury and traumatic brain injury claims are on the rise, and while science on that may be helpful, claims may become a serious issue as the insurance markets for this shrink and restrict coverage. Plaintiffs are looking to assign blame to coaches as well as medical professionals. Division III schools are also facing claims, where previously they had not.
- Physician misconduct is emerging as a new risk. Serial offenders may have created claims for multiple institutions as they change employment or freelance at other institutions. The tail, or years over which claims may be brought, for these matters may be very long.
- #MeToo means that any claim of sexual misconduct may balloon into a claim with several plaintiffs.
- Accessibility/ADA/504 claims, particularly for web and other electronic accessibility, are on the rise, with certain law firms trolling schools' websites for noncompliance.
- Institution closings may create complex claims, but since the institution is closing, it is a greater risk to underwriters. However, if the institution has arranged a merger with another institution, the risks to both schools is significant.
- Accreditation claims have been arising more frequently as schools expand or create new departments. They are likely to occur if the department isn't accredited and disclosure was not given to the students at the time of enrollment. Similarly, if institutions lose their accreditation and do not inform students, they may be liable for claims based on the failure to notify.
- Contingent BI losses arising from things such as cyber liability attacks that shut down key suppliers such as utilities, terrorist attacks or natural disasters, then damage transportation hubs and infrastructure that afford access to your campus.
- Domestic and international political risks that result in the loss of tuition dollars.
- Mushrooming cyber risks such as loss of functionality of an insured's technology platform (computer system) due to introduction of malicious cyber code/viruses, loss of customers as a result of reputational damage related to a covered cyber event, corporate identity theft, ad nauseam.

VI. After the Loss

One of the important resources that risk management brings to the educational institution's administrative team is information on emerging risks. Understanding how these risks can result in catastrophic claims can help the institution address them early by developing and implementing risk mitigation plans as part of the ERM or other risk management process.

We do not want to repeat the post-claim actions outlined in the hypothetical cases, but do want to highlight a few key points:

- Identify the root causes of the loss and go after them. Failing to address the causes of the loss will nearly always mean that the institution will face repeat claims.
- Perform a postmortem on major claims. Not only can this help identify root causes of the loss, but can also identify any issues that complicated the claim, worsened it or helped to ensure that it went smoothly. See the appendix for sample materials on conducting the postmortem.

VII. Appendix

Resources

Books

Dezenhall, Eric. *Damage Control: The Essential Lessons of Crisis Management.* Easton Studio Press, LLC. Kindle Edition, Revised and Updated.

Lentz, Daniel. *Business Interruption: Coverage, Claims, and Recovery*. The National Underwriter Company. Kindle Edition, 2nd Edition.

Selby, Judy. *Demystifying Cyber Insurance: For Data Breach and More: 5 Steps to the Right Coverage.* Judy Selby LLC, 2018.

Selby, Judy. *A Closer Look at Cyber Insurance: Exploring New Coverages, Including for GDPR and Other Regulations.* Kindle Edition.

Checklists

"Vehicle Accident Folder Structure" or "Catastrophic Claim Checklist," both developed by our Houston office in response to a university bus accident with death of student. Both checklists can be found in the appendix.

Security Breach Notification Laws by State

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html

https://www.itgovernanceusa.com/data-breach-notification-laws

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-guide-on-state-data-breach-laws.html

---

Incidents to Be Reported Immediately to Risk Management

Insurers are very interested in the early identification of complex claims. Within all liability policies there is a provision calling for the prompt reporting of occurrences involving certain types of injuries; some underwriters even provide a list of events or types of injuries. In addition to creating a contractual reporting requirement under the policy, these lists provide valuable insight into the types of events/injuries that insurance companies believe can lead to a complex claim. It is important to share your underwriter's list of these types of events/injuries with all persons who have reporting obligations under the policy terms and conditions. Risk management may want to develop their own contact list, to remind campus staff to provide immediate notification to the risk manager or general counsel. Here is a list of some types of events or injuries that might warrant highlighting:

- Fatality of any nature that is connected with the institution
- Injury resulting in major paralytic conditions, such as paraplegia and quadriplegia
- Amputation, permanent loss of use or permanent loss of sensation of a major extremity
- Serious burns
- Head or brain injury that results in severe symptoms (coma, seizures, aphasia)
- Allegations of sexual molestation, assault or rape
- A campus shooting or other major act of violence
- Any serious injury

Risk managers can create their own lists, which may reflect both underwriter requirements and/or institutional concerns.

Preparing for the Big, Complex Loss

Top 10 Things a Risk Manager Can Do Before a Loss

There are many nuances to every claim. It is hard to know what to do first. The best risk management strategy is always to be prepared for the worst while hoping for the best. Consider these actions that risk managers can take to be well prepared for the "Big One."

1. Know your insurance coverage (and how to access your policies when systems are down).
2. Know your insurance policies' claims reporting requirements, including excess policies.
3. Make sure that all supervisory staff know what a claim or reportable incident is and the office to which it must be reported.
4. Deliver awareness training across the institution on reporting of incidents and claims. This is especially critical for any positions that are a designated reporter under the insurance policies.
5. Pre-identify and use trained SWAT teams that can help identify and respond to complex claims at the very start of a claim or incident.
6. Engage in crisis/emergency response planning and drilling. For departmental drills, include an opportunity to drill on claim management. Don't overlook the risk management department in planning and running departmental drills.
7. Develop a method to track claims, including when they were reported to underwriters.
8. Get to know your institution's communications team and build a partnership with them so that when crisis communications are needed you will already know each other.
9. Have a good understanding of how and where records are stored.
10. Know is your carrier's approved outside counsel and who should represent the institution on what types of claims.

In addition to these preparatory actions, all institutions can engage in continual loss prevention activities and enterprise risk management to reduce the likelihood of catastrophic claims.

JANE DOE VS. UNIVERSITY

SAMPLE RETROSPECTIVE CLAIM REVIEW MEETING AGENDA

FEBRUARY 1, 2019

Attorney-client privileged communication

I. Brief Factual Overview

Plaintiff Jane Doe was employed as … in ABC Department for supervisor …. She started in …

II. Pertinent Legal Issues Presented by Litigation

- **A.** Claim: Race/national origin/pregnancy leave discrimination and retaliation, filed claim 7/1/20XX.
- **B.** Principal Defense: While John Doe's interactions with Plaintiff may not have been ideal, there was no evidence of discriminatory animus. Further, the issue of failure to mitigate damages arose because Jane Doe did not seek to return to active work until 20XY.

III. Final Disposition and Rationale

- **A.** Exposure: While many of the legal theories asserted by Plaintiff were not strongly supported by facts, there were several problems in this case that led to the decision to settle rather than litigate. They are as follows:
- **B.** Liability Assessment: See above.
- **C.** Rationale for Settlement: Supervisor … was not well liked in the department. Several employees interviewed spoke about his gruff nature. Plaintiff was a good employee who received favorable evaluations. While there was some indication that she did have excessive absences and often changed her flexible work week schedule because of her children's illnesses, thus causing disruptions at work, that issue could have been handled better by Supervisor. The two key factors that led to the decision to settle early in the discovery process were (1) the wording of Ms. Doe's complaint letter and (2) the manner in which Supervisor would present as a witness and his insistence that his interactions with Plaintiff were acceptable.

IV. Review of Process and Recommendations

What preventative measures can be employed?

V. Lessons Learned From This Case

What would or could we have done differently?

VI. Action Plan From Retrospective

Claim/case management

Supervisor training (general and department-specific)

Other

Retrospective Claim Meeting Action Plan

Category: Documentation IDENTIFIED AREAS	ACTIONS	CONTACT AND DEPARTMENT	TARGET COMPLETION DATE

Category: Communication IDENTIFIED AREAS	ACTIONS	CONTACT AND DEPARTMENT	TARGET COMPLETION DATE

Category: Policies IDENTIFIED AREAS	ACTIONS	CONTACT AND DEPARTMENT	TARGET COMPLETION DATE

Category: Other IDENTIFIED AREAS	ACTIONS	CONTACT AND DEPARTMENT	TARGET COMPLETION DATE

PROPERTY LOSSES—SUPPLEMENT

Build Claims Management Into Emergency Response and Business Continuity Planning

Business continuity planning is essential for managing and controlling property losses. If facilities are shut down, the institution needs to have plans in place to run payroll and continue some essential functions or you will have BI losses in addition to the physical losses. The following suggestions were made during the think tank:

- As you go through the planning for an emergency response, consider where damage could occur and what will be damaged. Is it really a good idea to have the animal research labs and quarters in the part of the building that will be the first to flood? Do you want to have expensive, sensitive equipment in an area that is prone to loss or exposure? Work with facilities and the rest of the institution to develop a plan to move these operations into less precarious surroundings. Put this on your enterprise risk list.
- Another aspect of the emergency response plan is to identify what building or buildings are most essential to the institution's operations or identity. Is there something on campus without which the school would lose significant enrollment or workforce? What buildings or programs need to go online first once a disaster has occurred?
- The No. 1 recommendation from the think tank participants was to run through your emergency response plan at least once a year and have response drills. Also, don't neglect the risk management staff—they need to drill on the risk management department's own response and recovery plan.
- Consider how, during the recovery process, you can keep essential personnel on campus to help manage the timely recovery. Does the institution have means to ensure that their families are safe so your essential personnel can be on campus to support the recovery efforts? Remember, families may include elderly parents and pets as well as children. Smaller institutions with limited staff will find this to be critical to their ability to respond with a full team.
- Multi-campus institutions need to be particularly sensitive to campus closure or curtailment, particularly if the campuses are in close proximity and may share staff or faculty. Consistency in the response to the locations will help manage student and parent expectations, as well as maintain good staff and faculty relations.
- Make sure that any new leadership is aware of the emergency response and business continuity plan, even if they haven't had an opportunity to participate in a drill. Each of them will have a role and responsibility in the plan—they need to know what that role is.
- Have a crisis communications plan in place for different types of situations, including for circumstances when cell towers are down and there are other barriers to communication due to a local or regional event.
- Consider when an event might happen and how the timing of an event might impact the campus. Is it just before the start of the semester? At the height of the academic program? Between semesters or over the summer? Evaluate how timing will impact enrollment and retention of the workforce, especially faculty.
- Establish the institution's replacement values, especially for research. See attached sample worksheet.

Valuing Your Research—Tracking Tools

Courtesy of Dartmouth College

Date:		Location/Name of Lab:	
Department:		Telephone:	
Professor/Researcher:		Timeline of Grant:	
Start Date of Research Contract:			
RESEARCH MATERIAL EXPOSURE:	PRIMATES	VALUE AT RISK*	$2,500,000

Potential Hazards Causes of Loss	Risk Level and Likelihood Rating	Action Plan to Mitigate Risk High Moderate Low	Responsible Party	Date Recorded

***How to Value Your Research**

- Cost of materials (including animals) involved in the research
- Funding source (grant proposal)
- Overhead charges—IT and administrative charges
- Equipment costs—if new equipment was specifically purchased for this research project
- Labor expended—breakdown by job type (researcher, technician, administrator, laboratory researcher/experimental costs) and percentage of time each person works on a specific research project

Sample Vehicle Accident Records Folder Structure

Following is a sample structure for organizing records associated with a serious or catastrophic vehicle accident (revised 08-22-2019).

- **PASSENGERS**
  - Passenger contacts
  - Medical contacts
  - Injury status updates (where properly released by patient)
- **ORGANIZATION CHARTS AND CONTACT INFORMATION**
  - Institution management and response teams
  - Gallagher team
  - Insurance carrier and adjusters
  - Legal counsel for institution
  - Legal counsel for victims/plaintiffs
  - Public relations and grief counseling services
- **INSTITUTION'S COMMUNICATIONS**
  - To passengers and families
    - Correspondence
    - Accident investigation
    - Filing claims on health plans
    - Other
  - Family support services
    - Expense payments
    - Counseling services
    - Academics
      - Current semester
      - Future semesters
    - Disability accommodations
      - Residential
      - Classroom
      - Other
  - To institution's community
    - Faculty and staff
    - Students
    - Institution's blog or other social media (e.g., Facebook, Instagram)
      - First days
      - Ongoing
  - Public relations
    - Advisor appointment
    - Institution's policy on internal communications (both privileged and public info)
    - Institution's policy on external communications (from perspectives of faculty, administration, passengers and families, other students; designation of Institution's spokesperson; etc.)
    - Media information and contacts
    - Press releases
    - Publications
  - Media coverage (with hyperlinks)
    - Print
    - Video
- **ASSISTANCE FUND**
  - Purpose
  - Eligible expenses
  - Communications
  - Banking and investment
  - Administration
- **CLAIMS INVESTIGATION**
  - Lead investigating agency
    - Personnel directory
    - Process steps and tracking status
    - Preliminary findings and reports
    - Final report
  - Institutions
    - Travel-related policies
    - Trip planning and approval
    - Driver credentialing and training
      - Drug testing, training, driving history, proof of CDL, etc.
    - Vehicle purchase and maintenance
  - Insurance carriers
    - Passenger statements
    - Witness statements
    - Accident reconstruction
    - Vehicle condition
    - Prior incidents (involving same or similar vehicle)
    - Black boxes

- Cellphone records
- Weather reports
- Vehicle and other property storage
- Photos
- Prior medical treatment, counseling histories (where properly released by patient)

- **LIABILITY CLAIMS**
  - Appointment of legal counsel (including letters of engagement, notes on scope of engagement, etc.)
    - Primary carrier
    - Excess carrier
  - Directory of legal counsel
  - Claims against
    - Institution and any institution personnel
    - Vehicle manufacturer
    - Vehicle maintenance
    - Vehicle dealer
    - Component manufacturers and assemblers
    - Other third parties
  - Releases of liability
  - Subrogation and liens
  - Legal research
    - Charitable immunity acts, etc.

- **INSURANCE**
  - Coverage
    - Summary (including erosions, benefits, liability, medpay, PIP, etc.)
    - Policies
      - Primary
      - Excess
      - Workers' comp
      - Travel accident
      - Other
  - Adjuster assignments
  - Written notices to insurers and brokers of incident and claims
  - Other

- **HUMAN RESOURCE MATTERS**
  - Employment records
  - Course and scope of employment determinations
  - Faculty return to classroom

Catastrophic Vehicle Accident Claim Checklist

A. Standardized Procedures

- ☐ Activate crisis team—key individuals on call 24/7 for notification in the event of a catastrophic claim
- ☐ Notification to claims adjuster
- ☐ Activate investigation team (generally safety personnel trained in proper documentation of catastrophic claims)
- ☐ Develop the litigation team (decisions-makers, corporate representative, etc.)
- ☐ Place insurance carriers on notice as may be applicable (including auto, workers' compensation, travel accident, excess liability)
- ☐ Retain defense counsel
- ☐ Notify OSHA
- ☐ Review injury benefit plan (including travel accident insurance) to determine death benefits and beneficiary status, if any

B. Information Gathering

Depending on who the involved parties are (e.g., employee, student or third party), the institution will want to begin gathering as much relevant information as possible, including:

- ☐ Date of hire
- ☐ Circumstances of the accident
- ☐ Was the death instantaneous or was substantial pain and suffering (or medical) associated with the injury?
- ☐ Copies of the company's standard operating procedures at the time of the accident
- ☐ Training records
- ☐ Operational and safety records
  - ☐ Driver logs
  - ☐ Maintenance records
  - ☐ Trip records
  - ☐ Bills of lading
  - ☐ GPS data (if applicable)
- ☐ Witnesses contact information and statements
- ☐ Evidence including photos, damaged vehicles, weather data
- ☐ Personnel file (including signed receipt for the injury benefit plan)
  - ☐ Determine other benefits or property held by company (AD&D, Life Insurance, 401(k), ESOP, etc.)
- ☐ Police interviews
- ☐ Police report

C. Potential Litigation/Arbitration

- ☐ Coordinate documentation with defense counsel
- ☐ Identify correspondence and documents as prepared in anticipation of litigation
- ☐ Comply with the duty to preserve evidence, (the institution has a duty to preserve any and all property, records, etc., that could be deemed evidence. Review all record retention policies; attorney approval must be sought prior to destruction of any property, records or documents.)

D. Family Visit

- ☐ Arrange immediate visit with family. (Try to have as much information as to available benefits [death, burial, and other benefits as identified above] when meeting with the family in the event they inquire. Money is generally not the topic to be discussed at this time, but it is best to be prepared. Do not delay the visit while waiting on this information.) Comments should or could address the following:
  - ☐ Sorrow over the loss
  - ☐ Company desire to help in any way possible with funeral arrangements
  - ☐ Employee's status as a participant in the plan
  - ☐ Researching other benefits
  - ☐ Make clear that the company is saddened by this loss, but do not make any statements as to fault with respect to the accident
  - ☐ Provide contact information to the family
- ☐ Identify survivors and dependents
- ☐ Identify estate administrator or distribution of assets

E. Memorial Services

- ☐ One or more representatives from the institution should attend the family's memorial service.
- ☐ The institution may wish to have its own memorial service for the deceased, but should secure approval from the family before proceeding.

Glossary

ADA/504 refers to the Americans With Disabilities Act/Section 504 of the 1973 Rehabilitation Act: https://dredf.org/legal-advocacy/laws/section-504-of-the-rehabilitation-act-of-1973/

Bordereau
A detailed note, memorandum of account or document, especially one containing an enumeration of documents. With respect to claims or incident reports, a list that captures essential information for a summary report to underwriters, including:

- Date(s) of incident
- Date of report
- Claimant identification (initials, number, name)
- Respondent identification (initials, number, name)
- Location of incident
- Brief description of incident
- Steps taken by insured

Builder's Risk Insurance
Builder's risk insurance is a type of property insurance that covers new construction or renovation. It is often purchased separately from an institution's property insurance because underwriters may need to underwrite and rate (price) the exposure as it usually is much riskier than ordinary property risks.

Business Interruption (BI) Insurance
Business interruption insurance (also known as business income insurance) is a subset of property insurance that covers the loss of income that a business suffers after a disaster. The income loss covered may be due to disaster-related closing of the business facility or due to the rebuilding process after a disaster. This type of coverage usually includes Extra Expense, funds that can be provided to the insured entity to pay for services or supplies that will reduce or eliminate a BI loss. For example, if a residence hall is left uninhabitable due to a fire, Extra Expense Coverage can pay for housing trailers on campus or hotel rooms for the students to eliminate any loss of income (tuition) that might occur if the students have no place to reside.

Captive Insurer
A captive insurer is generally defined as an insurance company that is wholly owned and controlled by its insureds; its primary purpose is to insure the risks of its owners, and its insureds benefit from the captive insurer's underwriting profits.

CIO: Chief Information Officer

CISO: Chief Information Security Officer

Contingent BI/Contingent Business Interruption
Institutions can sustain a BI loss if a significant or sole supplier experiences a loss that prevents them from providing the contracted goods or services to the institution.

EEOC: (U.S.) Equal Employment Opportunity Commission
The Equal Employment Opportunity Commission (EEOC) is an agency of the federal government, created by the Civil Rights Act of 1964 (Title VII). The purpose of the EEOC is to interpret and enforce federal laws prohibiting discrimination.

EH&S: Environmental Health and Safety

ERM: Enterprise Risk Management (Enterprise Risk and Compliance Management) is a process for managing an organization's risks.

FERPA: Family Educational Rights and Privacy Act
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

GDPR: General Data Protection Regulation 2016/679
The General Data Protection Regulation 2016/679 is a regulation in European Union (EU) law on data protection and privacy for all individual citizens of the EU and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

GETS Cards: Government Emergency Telecommunications Service Cards

GETS is a program of the Department of Homeland Security, Office of Emergency Communications that prioritizes calls over wireline networks. Users receive an access card (GETS card), which has both the universal GETS access number and a **Personal Identification Number (PIN).** To get priority access over cellular communications networks, you need to use the **Wireless Priority Service (WPS)** program. GETS and WPS can be used in combination. The GETS program is in effect all the time—it is not contingent on a major disaster or attack taking place.

High-Profile Individuals

These are individuals who, by reason of their position or fame, would be likely to gather a lot of publicity if there were to be a situation with which they were connected. Examples include the Chancellor or President of an institution; Trustees or Board Members; a famous professor or researcher; a famous student or parent.

K&R: Kidnap and Ransom

This is a specialized insurance product designed to aid organizations respond to the kidnapping of persons, including the arrangements for and payment of ransom. Malware or computer viruses can hold a computer system hostage until a ransom is paid; some K&R policies may respond to this situation.

NDA (Nondisclosure Agreement)

A nondisclosure agreement is a contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together. In the context of this paper, an NDA may be required as part of employment contracts, in institutional disciplinary proceedings, or in claims and settlement agreements.

Notice Requirement

All commercial insurance policies have a clause (term or condition) that stipulates that the insured must report the claim or, in some cases, the incident that could lead to a claim in a timely way. Most have limits on the time frame in which the insured can report, based upon when the insured became aware of the claim or triggering event. Failure to report a claim in accordance with the Notice Requirement may be grounds for denying the claim by the underwriters.

OCR: Office for Civil Rights

OCR's mission is to ensure equal access to education and to promote educational excellence through vigorous enforcement of civil rights in our nation's schools. OCR is the enforcing agency for Title IX and other laws pertaining to nondiscrimination in higher education.

PHI: Protected Health Information

Protected health information (PHI), also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care. Information is protected under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and revisions to HIPAA made in 2009's Health Information Technology for Economic and Clinical Health (HITECH) Act.

PII: Personally Identifiable Information

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. Under some laws, it may be defined as Name (first and last, or first initial and last name) plus any government-issued identity number (e.g., Social Security number, driver's license or passport number) or financial account number (e.g., bank, credit card or other account number).

Punitive Damages

Punitive damages can be awarded in addition to actual damages in certain circumstances. Punitive damages are considered punishment and are typically awarded at the court's discretion when the defendant's behavior is found to be especially harmful, performed with malice, or there was gross negligence or disregard for the potential for harm.

Reporting Office, Reporting Officer, etc.

The Reporting Office is the office that is responsible for reporting a loss to the insurer. A Reporting Officer is a position, defined in the insurance policy, that is required to report or ensure that a report of a claim is made to the insurer.

RMIS System

RMIS refers to a Risk Management Information System. These systems can be purchased or homegrown, and will typically track, at a minimum, claims and exposures. Some systems are designed to also track ERM processes and risk mitigation.

STEM: Science, Technology, Engineering and Math

SWAT Team (in Business)

SWAT team refers to a special-purpose team that is created for responding to/resolving a business-critical problem that cannot be and/or has not been resolved through the use of standard operating procedures.

TBI: Traumatic Brain Injury

The CDC defines a traumatic brain injury (TBI) as a disruption in the normal function of the brain that can be caused by a bump, blow, or jolt to the head, or penetrating head injury.[2]

Tickler Process

A tickler file is a group of files that are in order by the date upon which a certain action is needed. When used correctly, it can provide ready access to tasks that need to be accomplished on a daily basis.

Title IX

The U.S. Department of Education's Office for Civil Rights (OCR) enforces, among other statutes, Title IX of the Education Amendments of 1972. Title IX protects people from discrimination based on sex in education programs or activities that receive federal financial assistance.

TPA: Third-Party Administrator

A business that provides claims administration services to an insurer or self-insured entity. Some TPAs also handle the transactional aspects of managing employee benefits.

University Business Incubators

A university-sponsored organization or department that provides support, such as expertise, space and resources (e.g., computing networks, 3D printers) to students and possibly others (staff, faculty, other applicants) in exchange for a small royalty if the entrepreneur is successful in launching their business and earning a profit.

Waiver of Subrogation

Subrogation is a term describing a legal right held by most insurance carriers enabling them to make a claim against a third party that caused an insurance loss to the insured. This is done in order to recover the amount of the claim paid by the insurance carrier to the insured for the loss. For example, an auto insurer will file a claim against the insurance company of the party responsible for a car crash to recover their loss. A waiver of subrogation is an endorsement to or clause in an insurance policy that permits the insured to enter into a contract that waives the right of the insurer to file a claim against the contracting party for their responsibility for a loss, as long as the waiver was made prior to a loss. This is common in construction projects where one policy covers potential property losses, and in contracts where the two parties share equal responsibility for the work, activity or event. It can also refer to the clause in the contract between the two parties in which there is a unilateral or bilateral waiver made.