

HUMAN CAPITAL RISK:

THE CRITICAL ROLE OF HR THREAT ASSESSMENTS



**LOWERS
& ASSOCIATES**

International Risk Mitigation Partners

A Lowers Risk Group Company

Today's business environment is uniquely unpredictable. Every day we hear about and see things that "could go wrong" actually going wrong—surprising the organizations, institutions, and people most affected.



“Almost everything that can go wrong in a business has a human capital component.”

— DAVID CREELMAN OF CREELMAN RESEARCH

David Creelman points out the critical importance of managing human capital risks. You can have the best processes in the world (on paper) but if you have the wrong people in place, risk can turn into loss fast. When those risks aren't even on your radar, the losses can be devastating.

Here are a few examples of common human capital risks that become losses:

- A key high level manager moves away to take care of his mother and easily gets another job working remotely, leaving a huge hole in critical operations.
- A technology update is needed but the IT manager is too swamped and misses the latest.
- A 'trustworthy' receptionist (or director) has access to keys and easily steals products, assets, or money.
- A couple heading for a celebratory dinner hands over their keys to a valet who now has their registration and garage door opener. In this case, the combination of a low wage, low skill employee, and access to others' material goods is a recipe for trouble.
- A CFO receives an email that appears to be from the company President, asking them to wire a large sum to money to an unfamiliar account, ostensibly as payment to a vendor. What they don't know is that the email was spoofed and sent by a would-be thief.
- An armored car company, short-staffed at a small branch, allows a single employee to operate a route by himself with unrestricted access to the cash being transported. One day, after several customers call the branch to report that they haven't been serviced on time, the truck is found abandoned with hundreds of thousands of dollars in cash missing and the driver nowhere to be found.



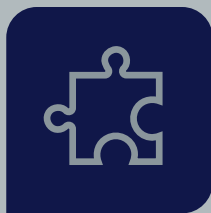
NEVER UNDERESTIMATE HUMAN CAPITAL RISK.

A moniker worth repeating and heeding.

Risk is a natural component of doing business, and one that it isn't relevant to just a single part of the company or organization. Human capital risk affects everyone and must be managed and mitigated constantly. Rigorous risk management is a responsibility crossing all department lines.

Human Resources (HR) generally carries the load for making sure that the 'Human Capital' component of a company or organization hums—that it is successful and productive—but HR as a company function is often held separately from Enterprise Risk Management (ERM). This is a short-sighted view that can result in disaster. Knowing your risks is the first step in mitigating them. Knowledge is power, and the threat assessment is the source of your power when it comes to human capital risk management.

When it comes to Enterprise Risk Management (ERM), a majority of risk is directly related to the human capital (the people!) who are fulfilling business objectives—from the C-suite to the mailroom.



“People are at the core of each major risk. If not as part of the problem, then as part of the solution.”

— DELOITTE, 2012 REPORT

Human capital risks commonly stem from these five critical areas:



Complacency



Turnover



Occupational
Fraud



Catastrophic
Workplace
Events



Negligent
Hiring or
Retention

“Managing human capital risk is important to success, but organizations aren’t doing anything about it,” says Ellen Hexter, senior adviser on ERM for The Conference Board.⁵ Deloitte, likewise, reports in their 2014 Risk and Regulatory Talent Survey, “HR risks continue to be absent from the risk management framework. Only 36 percent of survey respondents indicated HR risks as included in the risk management framework, suggesting an opportunity to formalize the dialogue between talent people and risk people.”⁷

Today, many companies understandably choose to prioritize investments in capital assets or technology, often compromising with insufficient planning, education, or training programs. As a risk manager, it’s important to consider the full range of costs and benefits of all assets, including considering whether or not staff can (or will) deploy investments properly. It is also critical to take into consideration the ongoing state of human capital as a whole, as all kinds of assets change regularly, including your staff members themselves. Errors in judgment or simply missing out on the most up-to-date technology, operations, or training can all cause losses.



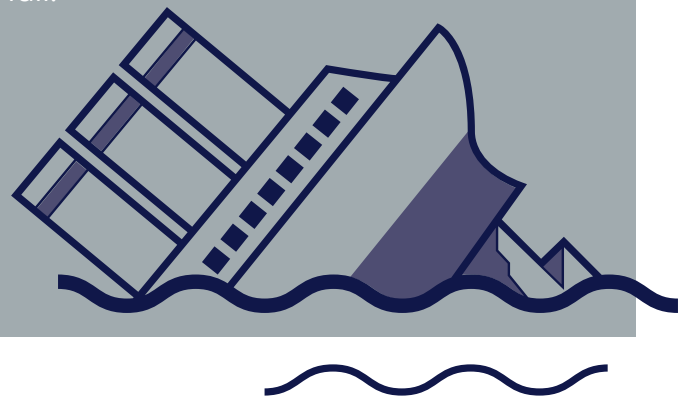
DON'T LET YOUR UNKNOWN RISK SINK YOUR STRATEGIC SHIP

The sinking of the Titanic is a classic example of what can happen when human capital risks are unknown or ignored. In this extreme case, 1,502 people died in one of the worst maritime accidents ever. There were risks that could have (and should have) been detected. Some risk factors were even known and tragically dismissed. In hindsight, more rigorously assessing and managing the Human Capital Risk(s) could have averted disaster and possibly saved lives. For many decades now the contributing factors of this incident have been studied in the hopes of preventing similar losses in the future. These findings help guide companies today in mitigating risk and maximizing stability and success.³

Here are some factors that went awry with the Titanic where human capital was involved:³

- According to the US Senate inquiry, the ship's speed was excessive, considering its size and steering capabilities.
- Neither Captain Smith, nor the ship's owner, Mr. Ismay, heeded multiple warnings of ice flows sighted in the crash vicinity—relevant info provided by local sources.
- A key factor in the Titanic's sinking was its core design. While the ship's architects boasted a 'watertight' design, once punctured, multiple side-by-side compartments filled and held water, making the ship's base heavier than anticipated.
- Construction choices included materials for the hull and rivets that became brittle when cold, causing structural damage in the icy waters of the North Atlantic.
- The crew had not been adequately trained in carrying out a full-scale evacuation. Numerous officers were not told how many people they could safely put aboard the newly designed lifeboats. As a result, the crew launched many of the lifeboats barely half-full.
- While Captain Smith was an experienced seaman, he had not headed a ship of the size and complexity of the Titanic.

And the list goes on...



As evidenced by the Titanic disaster, both individual human error and staff or workflow management, if not properly evaluated as part of personnel risk, can significantly affect the results of any major operation. Understanding real risk, as with any strategic objective, can only be done by examining every angle and identifying your unique issues before potential problems become real losses.



THREAT ASSESSMENT, WHAT'S THE BIG DEAL?

WHAT IS A THREAT ANYWAY?

Human capital risk is defined as any human resource or personnel-related risk that creates vulnerability to an organization's ability to achieve its strategic and operational goals or objectives. It can also be viewed as the likelihood of loss of anything having value, including people, facilities, information, equipment, and reputation. In other words, risk is the probability that a particular threat will exploit a given vulnerability, leading to an unwanted result.

WHY THIS MATTERS

When you think about HR, "risk" may not be the first word that comes to mind. The word may elicit thoughts of theft, cyber breaches, hazardous spills, or other such obvious dangers. Recruiting, benefits administration, or continuing education may not fit into any perceived risk category. This is, of course, entirely understandable on its face.

Human capital is, however, one of the most pressing corporate risks and continues to appear on the Government Accountability Office (GAO)'s high risk list as a result. Limitations in corporate budgets, changing regulations around retirement, and widening skills gaps for key positions all limit HR's ability to find, attract, and keep the best people in key jobs, doing the most efficient work in the most strategic timing.⁵ The unacceptable alternative is underperforming or settling for unreliable or even untrustworthy personnel.

Human capital management or human resource management is more than simply attracting and retaining talent. Risks can also be associated with operational systems, financing, safety, or even strategic direction. It is important to thoroughly understand both the needs and risks associated with all aspects of your human capital, especially where employees intersect with the public. Many factors must be considered within the ERM program to understand the full risk picture of a company. Only then can controls and systems be established to proactively prevent, minimize, or manage human error and maximize success.

SCOPING RISK



A recent poll of 500 C-suite and board-level executives found “talent and skills shortages” to be the No. 2 risk facing businesses, up from 22nd place in 2009. The No. 1 risk noted in the poll was “loss of customers,” while “reputational risk” was No. 3.⁴ All of these risks impact the bottom line and should be factored into a healthy ERM program.

Even prepared companies with thorough ERM programs may not be considering all relevant aspects of staff needs or work-flow management issues. Have you included these recognized principles of human capital risk management?²

- **Creating and protecting the value of an organization**
- **Efficiently leveraging existing human resources**
- **Proactively addressing areas of uncertainty**
- **Making allowances for human factors and fallibilities (balance)**
- **Balancing factors of cost—both financial and non-financial resources—with loss potential**

The cheapest option is not always the most cost effective one. It may in fact expose the business to additional risks.

THE DEVASTATING OSTRICH EFFECT: AVOIDING ASSESSMENT CAN COST

Some organizations simply do not realize that the HR department's responsibilities actually do overlap the risk management arena, often with considerable impact. In these cases, working cooperatively across departments can immediately result in a quality assessment, putting your company on the road to proper planning.

In other cases, however, organizations may fail to complete (and/or update) their Human Capital Risk Assessment for reasons that are worth uncovering in the interest of reducing risks and possibly even saving lives.

Here are some common reasons why a company or organization may avoid a human capital threat assessment.



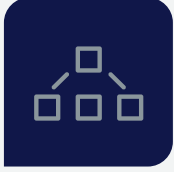
1. RESULTS

The company (usually trickling down from the C-suite) is primarily focused on bottom line success. This means pushing for profitability, performance, or status at the expense of worrying about 'what if' scenarios. A company may choose to invest in systems that promote efficiency rather than considering safety, retention, morale, or other risk factors.



2. TIMING

Sometimes companies adopt a holding pattern, 'waiting' for something to happen in order to trigger the assessment. Waiting for a vote on policy that could affect relevant procedures is one such example. Or perhaps the company is in the midst of a process to select a vendor (insurance, security, technology). Perhaps the timing/review cycle of the assessment itself could be outdated—an annual review for example, for a business that sees frequent turnover or technology updates.



3. MANAGEMENT STYLE

Sometimes management is the problem, operating from a posture of avoidance. While no one would argue that the amount of responsibility and oversight expected from businesses today is enormous, it is just that—RESPONSIBILITY. Anticipating what could impact your business and taking measures to mitigate risk is your responsibility. When you take it on and put measures in place, the effort is one that pays off with a ripple effect—one you'll hopefully never actually be able to measure.

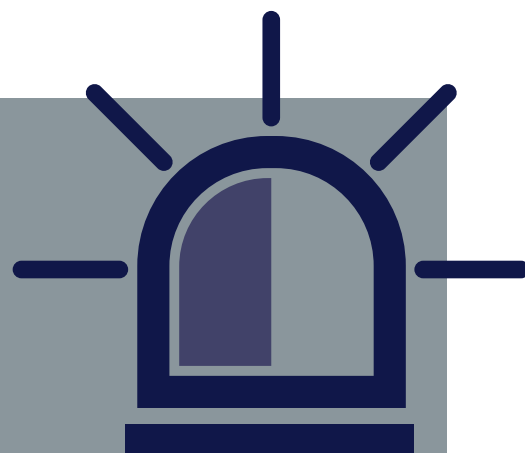
A short-sighted perspective can be even worse than straight avoidance. For businesses that get hit with an incident they don't even see coming, the loss can be utterly devastating. In order to assess, you have to be willing to admit that your business can be at risk. Like David Creelman said, "Almost everything that can go wrong in a business has a human capital component." It's always worth taking a long view and making the effort to assess.





CONSIDER THIS PERSPECTIVE FROM A MORE RECENT INCIDENT: ORLANDO'S PULSE CLUB SHOOTING.

When the tragic shooting happened, a multitude of people beyond the victims themselves were immediately impacted: club executives and employees, first responders, neighborhood businesses, local community organizations, hospital employees, media personnel, and all the families and organizations that employed those victims were immediately and intensely affected by the crisis.



Answers to certain questions were immediately required:

- How do we know what is happening at the location, en route and in the hospital(s)?
- What is the precise influx of patients, how do we assess the medical needs of, prioritize, and manage the volume of patients?
- What communication is flowing between multiple organizations (including the media) and are there any legal or social ramifications that need to be addressed immediately?
- What are the immediately relevant HIPPA regulations and questions and what can we do about them to allow for the most generous communication across all channels?

Without some quality risk planning that was luckily in place, this crisis could have been even more devastating. If additional planning had been in place, could more lives have been saved?

The Orlando first responders, along with the Orlando Health Hospital Systems, had some level of planning in place and did their best to manage the chaos. Here are some examples of steps taken.

- They knew how many staff and surgeons were available so the human resources could be organized quickly and effectively as soon as they determined what the situation was.
- The hospital locked down any extraneous operations including visitation until the crisis was under control.
- The hospital directed blood donors to nearby donation centers rather than adding the traffic and resource expenditure to the hospital facility.
- Orlando Mayor Buddy Dyer asked the White House to waive HIPAA regulations to allow local hospitals communicate with victims' families.

One evolution that occurred as a proactive outcome for future planning is that all first responders are now being more extensively trained in tourniquet protocols to potentially save more lives in a case of extensive bleeding.

While the Orlando shooting was an extremely devastating incident, it reminds us that planning and assessing risk with the goal of mitigating it can, in a best case scenario, be a subtle way to build trust and loyalty in all levels of an organization but potentially, in a worst case scenario, can save lives and unify an organization or even a community.

A SIX STEP PLAN TOWARD PROACTIVE PROTECTION

If there is any good news when talking about risk management, it's this: *with a thorough assessment and proactive planning, risks can be mitigated.* Effective threat assessment occurs within a context of safety. When your organization is ready to establish and promote a culture and climate of safety, respect, and emotional support, then the organization can proactively reduce or even eliminate the likelihood of violence and loss. Profit, reputation and even lives can be saved.¹

Here are the best practices of a Human Capital Threat Assessment.



1. IDENTIFY THREATS

Consider both existing and emergent threats.

In this first step you need to think outside the box about what threats could look like in your industry at this time or in the near future. The ones that bite the hardest are the ones you didn't even know about. Don't be caught off guard—get creative and curious. Your industry may be impacted similarly to what has occurred in other industries—pay attention and don't be afraid to consider how an event or cultural shift could impact your human capital equation.



2. CATEGORIZE

Determine internal vs external sources of threats and how to mitigate them.

This is a time to look at what is already in place and to begin assigning mitigation measures into operations. You can't always prevent threats from happening, but it is often possible to lessen their impact.

When it comes down to it, it's your job as a risk manager to mitigate risk. Maybe this means installing bullet-resistant glass or increasing your insurance coverage. Consider your options and look at what makes the most business sense.



3. EVALUATE

Assess the likelihood and outcome/ramifications of each risk.

While insurance covers many things, there are related, intangible costs that can easily be overlooked, such as your reputation or changes to the industry. A single significant incident can be enough to trigger these shifts. When it comes to Human Capital Threat Assessment, this evaluation process is most effective when conducted across multiple departments so as to obtain a full perspective.



4. PRIORITIZE

Recommend proper security and defenses to address your specific threats.

Not all threats are equal. Threats must be examined and prioritized based on their likelihood and the correlate potential losses (consider people, profits, brand, market position, reputation) in order to determine an effective mitigation strategy. You must walk the line between the cost of risk management and the cost of a crisis.

Note: As discussed before, many companies minimize ERM as it relates to HR. When factoring in budget considerations for key corporate strategic priorities, Human Capital Risk is worth including as a line item and earnestly weighing as you establish priorities.





5. AUDIT & TEST

**Regularly check for suitability and employee compliance.
Also, test measures for effectiveness.**

Complacency can be a big issue that nullifies risk management efforts. Simply having all of these measures in place on paper is worthless without the proper execution.

Take for example, the owner of a small jewelry shop, who, at one point added all the physical security measures recommended to him—full alarm coverage, decorative security bars on his windows and doors, and a more than adequate safe to store his valuable inventory. He operates in a low-crime area, and can't remember the last time he's heard about a robbery, a burglary, or even vandalism in the area. Over time, he becomes complacent to the belief that nothing will ever happen. He may still set the alarm system daily, but he's not so consistent on securing the inventory in his safe every night—it just takes too much time to pull it out and put it in the safe, only to have to put it all back out on display the next morning! Was he just "unlucky" that a few weeks later, a group of thieves backed a stolen pick-up truck through the front door, smashed his display cases, and made off with thousands in jewelry in under three minutes? And yes, the alarm activated!



The lesson: If you don't periodically check the mitigation measures and wrongly assume that they are still effectively in place, you may as well not have mitigation measures at all.



6. MONITOR

Evaluate, monitor, observe, and assess for new or evolving threats and to optimize your risk mitigation program.

Criminals know how to get around loss prevention measures, which is why you need to constantly monitor their techniques and assess your vulnerabilities to them. When dealing with risk management, it's all too easy to find yourself mired in byzantine security concerns that are specific to the way you've always done business. The reality is, however, that attacks don't have to be complex to be effective. This is a time to utilize the law of parsimony—the simplest answer is likely the right answer. If you don't, a criminal will.



Take, for instance, the popularity of social engineering “hacks” which completely bypass even the most advanced computer security programs. A criminal, rather than trying to hack into your company's internal network, will simply call the office pretending to be with the IT department. They'll introduce themselves to a hapless employee and ask for their log-in info so that some tech-jargon problem can be dealt with. The employee will hang up satisfied that they've helped the company and, just like that, the criminal now has an open door to your entire electronic database. Too many companies invest in high-level protection and fail to prepare their staff to deal with attacks as simple as this.

Approach risk from every angle, keep abreast of current risk trends, observe how criminals are striking other businesses, and actively use that information to ensure that you don't make the same mistakes.



THESE 6 PRINCIPLES REFLECT AND SUPPORT THE NEED FOR THOROUGH THREAT ASSESSMENT¹

- 1 Violence/crime is often the end result of an understandable, and oftentimes discernible, process of thinking and behavior.
- 2 Violence/crime stems from the interaction between a person, a situation, a setting, and a target—any and all of which can (and should) be monitored and managed.
- 3 An investigative, skeptical, inquisitive mindset is critical to any successful threat assessment.
- 4 Effective threat assessment is based on facts rather than characteristics or “traits.”
- 5 In a threat assessment, consider whether a situation could eventually pose a threat, not only whether the situation is currently presenting as a threat.
- 6 An “integrated systems approach” should guide threat assessment investigations. In a threat assessment, bits of information might be viewed as pieces of a puzzle. Each bit may appear inconsequential or only slightly worrisome by itself. When the pieces are put together, however—as oftentimes has occurred in “after the fact” analyses of an incident—the behaviors and communications of a perpetrator may coalesce into a discernible pattern that indicates a threat.

In many school attacks, for example, information existed within the school and community that might have alerted authorities to the risk of attack posed by a particular student.

Of course, one important factor of the human capital risk assessment is the nature and capability of the team implementing a strategic initiative at any level of the company. “One of the ways in which you can manage and mitigate human capital risk is if you can hire people with learning agility, who can figure out the best approach in an ever-changing situation,” says Orlando D. Ashford, senior vice president and chief HR officer at New York-based Marsh and McLennan Cos. Inc.

“Getting [talent] here and getting them to stay is only half the battle – it won’t do much good if they’re not being optimized,” Ashford says. “Ensuring talent is optimized and engaged so they are thriving, not just surviving, is critical in this global economy.”⁴

“You always want to make sure you’re building on employees’ capabilities, rather than just letting [development] happen,” says PepsiCo Executive Vice President and Chief People Officer Cynthia Trudell.

QUALITY QUESTIONS TO GET YOU STARTED ON YOUR THREAT ASSESSMENT:

Have you considered...

- 1 How human capital risks factor into or compare to other corporate risks?
- 2 Which human capital risks you need to actively manage, insure, and/or prevent?
- 3 Whether your benefits program provides sufficient protection for key personnel?
- 4 Whether your benefits program allows for the required attraction and retention of key personnel against that of your peers?
- 5 What is or could be targeting your industry and your organization that could cause disruption or loss?
- 6 How ‘agile’ your staff is, particularly in higher risk departments/roles?



GETTING IT DONE IS THE KEY. YOU DON'T NEED TO KNOW IT ALL OR DO IT ALONE

The most important part of conducting a threat assessment is making sure that it gets done. If you have no ERM program at all, or if your ERM doesn't include a human capital risk component, then your risk management program is incomplete, leaving you and your company or organization at risk.


Because global risk is constantly changing and because it is imperative to be able to respond effectively (and fast!), many companies choose to rely on the specialized expertise of a strategic advisor who is versed in potential disruptions, market issues, or cross industry trends. Global risk consultants can help navigate challenging territories such as changing reporting requirements or regulatory compliance issues, along with planning and implementing proven mitigating measures.

At Lowers & Associates, our comprehensive threat assessment program covers the spectrum of risk management and mitigation. From threat identification and evaluation to mitigation and ongoing monitoring, our program will help keep your risks in view and in check. Knowledge is power. Give yourself the gift of support and get your threat assessment done. Contact a Lowers risk management consultant today for more information or to schedule a conversation.



**LOWERS
& ASSOCIATES**
International Risk Mitigation Partners

lowersrisk.com | (540) 338-7151

- 
1. *US Secret Service & US Dept. of Ed Threat Assessment Guide*
 2. *Human Capital Risk - Risk Considerations Bulletin*
 3. *Evaluating Human Capital Risk: A Titanic Effort*
 4. *Human Resource Executive Online: The Human Risk Factor*
 5. *Ernst & Young Human Capital Risk Management*
 6. *Lowers Risk Group Threat Assessment Blog Post*
 7. *Deloitte Risk, Culture and Talent in Global Financial Services*
 8. *Deloitte 2012 Leap Ahead Report*
 9. *Lowers Risk Group HR-ERM Whitepaper*