****

**WikiRisk**

**12 pack**

**Aging Workforce**

**STRATEGIC RISK –** Organizations will need long term strategy to deal with the complexity of this risk.  It will impact the value of a company because of the lack of internal perpetuation possibilities, as well as increased costs and HR issues with the aging workforce.

**BUSINESS RISK –** Business risks will be financial costs to the daily operation, lack of innovation or ability to innovate quickly, difficulty of attracting younger talent, time off (vacation and sick), absenteeism, presenteeism, and retirement frustrations for clients, employees, and the employee.

**HAZARD RISK – Not Applicable**

**Methods to Manage This Risk**

**PREVENT**: Build strategies for proactive planning with employees at all ages to help with financial objectives (financial health) as well as retirement planning.  Make sure all HR items are in place so that age discrimination law suits are not filed.  Create mandatory age retirements.

**MITIGATE**: Strong over site to the process is critical.

**TRANSFER**: Not always possible, but go to employee leasing.

**FINANCE:**Life insurance, disability insurance, 401k funding.

**ASSUME:**This is one risk you don't want to assume or absorb the cost.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Loss of productivity=$
* Increased Sick Time
* Employers unprepared for aging population retirement
* Aging population unprepared for retirement
* Over 100 million baby boomers in the US and Canada
* Workforce needs of employers due to vacancies
* Baby boomers control 80% of personal financial assets and over 50% of discretionary spending power. In July 2011, they were responsible for more than 50% of consumer spending.

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Create productivity model by age group
* Healthcare premium increases
* Cost of not perpetuating because no spots available for future owners
* Analysis of Paid time off & Sick Time to determine cost by age group
* Determine the cost of the business if it does not perpetuate.
* Losing the intellectual capital of this group when they leave.

**SOLUTIONS:**

* Wellness strategy targeted toward older population
* Financial wellness strategies
* Exit strategy planning
* Have system in place for older population to remain productive in workplace environment
* Work on a better understanding of personalities between the generations for better communication (see generational characteristics attachment)
* Capture intellectual property through workbooks, videos, or interviews.

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* How are you currently managing your aging population?
* What are you doing currently to maintain productivity within the aging population of your workforce?
* Are you aware of the average age of your workforce?
* When was the last time that you analyzed your Sick/Time/PTO for trends?
* How are you helping your aging population prepare for retirement?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.bcg.com/media/PressReleaseDetails.aspx?id=tcm:12-93373>
* <http://www.economist.com/node/15450864>
* <http://www.globalhrnews.com/story.asp?sid=1061>
* <http://www.dol.gov/odep/pdf/NTAR_Employer_Strategies_Report.pdf>
* <http://www.theiionline.com>

**Social Media Risk - External/Internal**

**STRATEGIC RISK –**Not managing the implementation of a social media strategy can damage your brand in the marketplace, impacting the ability to obtain customers and acquiring talent in the future.

**BUSINESS RISK –**If managed incorrectly, can impact day-to-day operations due to privacy concerns, lower morale, discrimination and defamation claims.

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Strategies include: make sure that antivirus and anti-malware controls are installed and updated regularly (with regular training on policies and procedures), establish clear policies for employees on what information can and cannot be shared on social media outlets (to protect information and brand), create the ability to capture all employee communication using company data or systems. Another potential prevention strategy that may need to be addressed is the client expecting a quick response due to the social media and information age. Clearly state expectations for a response time.

**MITIGATE:** Have a response plan alerting any customer whose information may have been compromised and detailing what your firm is going to do about it. Establish regular communication strategy with clients, media, and employees as to the progress on cleaning up breach.

**TRANSFER:**Outsource social media web presence and data collection to an outside firm who manages brand, data collection, and data monitoring.

**FINANCE:**Cyber liability policy covers limited cyber risk but does have a response/public relations trigger that offers quick response procedures in the event of a data breach. Reputation loss can be financed through a micro-captive (831b) arrangement.

**ASSUME: I**dentify the cost of a data breach or a damaged brand due to a rogue employee and prepare financially for the impact to the business.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Brand new risk
* Generating privacy, defamation, discrimination, and other claims
* NLRB active in protecting complaining employees
* Difficult to monitor and control
* Lack of training and policy development
* Lack of coverage

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Decrease in employee productivity if using of social media no usage policy (21% of employees in a recent survey admitted to spending at least five hours per week on social media).
* Cost of employment related litigation costing on average $12,000 per case (not including time involved).
* Damage to brand due to complaining employees. One company lost over $1,000,000 in value overnight due to an employee doing foolish things on YouTube while on the job.

**SOLUTIONS:**

* Develop policies and procedure with employee input
* Monitor web and social media activity
* Promptly respond to complaints, breach of privacy, etc.
* Access to expert advice
* Proper insurance coverage
* http://blogs.hbr.org/cs/2013/03/hack-proof\_your\_companys\_socia.html

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* Tell me about your current social media policy?
* When was the last time you reviewed your current insurance coverage to determine if it includes social media risks?
* How do you monitor the time that your employees spend on social media while at work?
* How do you monitor what your employees are saying online about your company?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.x1discovery.com/social_media_cases.html>
* <http://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work/>
* <http://thebetterleyreport.wordpress.com/category/cyber-risk-insurance/>
* [www.socialmediarisks.com](http://www.socialmediarisks.com/)
* http://blogs.hbr.org/cs/2013/03/hack-proof\_your\_companys\_socia.html

**Cyber Liability**

**STRATEGIC RISK – Not Applicable**

**BUSINESS RISK –**If a cyber loss occurs within your business, the day-to-day operations of the company will be severely impacted while spending the time and resources to contain the breach and working with customers effected.

**HAZARD RISK –**Could have a damaging impact to hardware and software currently in use in the business.

**Methods to Manage this Risk**

**PREVENT:** strategies include: make sure that antivirus and anti-malware controls are installed and updated regularly (with regular training on policies and procedures), establish clear policies for employees on what information can and cannot be shared on social media outlets (to protect information and brand), create the ability to capture all employee communication using company data or systems. Another potential prevention strategy that may need to be addressed is the client expecting a quick response due to the social media and information age. Clearly state expectations for a response time.

**MITIGATE:**Have a response plan alerting any customer whose information may have been compromised and detailing what your firm is going to do about it. Establish regular communication strategy with clients, media, and employees as to the progress on cleaning up breach.

**TRANSFER:**Outsource social media web presence and data collection to an outside firm who manages brand, data collection, and data monitoring.

**FINANCE:**Cyber liability policy covers limited cyber risk but does have a response/public relations trigger that offers quick response procedures in the event of a data breach. Reputation loss can be financed through a micro-captive (831b) arrangement.

**ASSUME:** Identify the cost of a data breach or a damaged brand due to a rogue employee and prepare financially for the impact to the business.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Hackers gaining access to confidential data
* Employee loses data while off-site
* Employee steals data or uses data illegally
* Firewall security
* Lawsuits
* Loss of reputation
* Loss of clients
* What are hackers looking for: **personal identification** (name, social, credit card, benefits info, etc.), **processing power**(unused space in the business' server system to distribute botnets, illegal storage, etc.), **customer data** (emails, names, account numbers, etc.)

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Cyber crimes cost companies $214,000 on average, per attack.
* Smaller-sized organizations incur a significantly higher per capita cost than larger-sized organizations, per record stolen ($1,088 versus $284).
* Average time to solve a cyber attack, from an outside intruder, is 18 days (with full attention paid to the issue).
* Malicious insider attacks can take more than 45 days on average to contain.
* http://www.sicherheitstacho.eu/
* Data Loss Cost Calculator: http://www.tech-404.com/calculator.html

**SOLUTIONS:**

* Systems in place to identify cyber liability risk (annual audit to find key vulnerabilities internally and externally)
* Firewalls and Software Security Updates regularly
* Anti-virus systems on each computer
* Employee training on suspicious attachments and other cyber liability issues (password structure, what is a bonnet, how to identify a hacker, etc.)
* Cyber liability policy for every employee
* http://www.fcc.gov/cyberplanner (customized plan for a small biz)

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* What would a cyber liability lawsuit cost your company?
* How many of your employees access your server from home?
* What policy or system is in place to prevent family members from accessing sensitive data?
* What policy do you have in place to track sensitive data?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.infosecurity-magazine.com/view/25966/cybercrime-costs-companies-an-average-of-214000-per-attack/>
* <http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf>
* http://www.sicherheitstacho.eu/
* http://www.fcc.gov/cyberforsmallbiz

**Workplace Safety**

**STRATEGIC RISK –**Lack of safety on the job can impact the reputation of the company and lead to loss of future contracts.

**BUSINESS RISK –**Injured employees cost the day-to-day ops and profitability of the company.

**HAZARD RISK –**Employees injured on the job create a physical loss in the company by taking away the physical asset that is the employee.

**Methods to Manage this Risk**

**PREVENT:** Accidents in the workplace occur for 3 primary reasons: unsafe acts, unsafe conditions, and uncontrollable events. Prevention is achieved with the elimination of the hazard, substitution of the hazard with another process, engineering controls, administrative controls, PPE utilization, and regular training.

**MITIGATE:**Any safety program must specify steps to minimize injury cost. Establish how incidents are reported, proper steps to receive medical attention, and how the injury is to be followed up on to get the injured party back to work. Report all incidents, including near misses, to improve the effectiveness of the safety program. Conduct regular training on how to handle an injury and how to perform a post-accident investigation.

**TRANSFER:**Contract with an employee-leasing firm who assumes all liability injury losses.

**FINANCE:** Workers compensation for an injured employee. General liability for bodily injury to others.

**ASSUME:** Understand the cost of lost productivity, poor morale, and lost sales due to higher frequency and severity of accidents. Also understand that your competitors who are implementing safe work cultures are enjoying a competitive edge due to lower costs associated with the above.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Safety issues go unchecked and lead to an accident or injury
* Without employee buy in, safety does not become cultural within the organization
* Safe work environment is at risk

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Direct costs of a lost work day injury according to OSHA = $28,000
* Direct Cost of a reportable case without lost work day = $7,000

**SOLUTIONS:**

* Development of a Safety Committee
* Installation of a safety culture

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* Share with me what you are doing to develop and maintain a safety culture within your organization.
* How effective is your safety committee?
* What are the biggest safety issues you deal with?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.osha.gov/SLTC/etools/safetyhealth/mod1_estimating_costs.html>
* <http://www.ccohs.ca/oshanswers/information/injury_statistics.html>

## Employee Dishonesty & Crime

**STRATEGIC RISK – Not Applicable**

**BUSINESS RISK –**When a fraudulent event occurs within a company, it impacts the daily operations by taking attention away from the making of money and to the securing of money.

**HAZARD RISK –**Creates a physical loss by the inability to access capital.

**Methods to Manage this Risk**

**PREVENT:** strategies include hiring an independent auditor to monitor bookkeeping operations, installing security cameras at or near cash registers, personally overseeing financial transactions within the company to make sure nothing seems out of line, checking prospective employee backgrounds to make sure they do not have a history of stealing from others, conducting surprise audits of the books from an outside party, create a culture of understanding that fraud will not be tolerated and it can be reported anonymously if someone is suspected of theft, and making sure that employees take regular vacations (because this is when fraud is most often discovered).

**MITIGATE:**When a fraud is discovered, the company must act quickly to report the individual to the authorities, notify other employees around their job responsibility and notify the insurance company of a potential loss. The company should immediately begin an internal investigation to determine the exposure of the individual committing the fraud as well as exposure to other employees following a similar track.

**TRANSFER:**Outsourcing the bookkeeping function could transfer the risk to the hired firm as they may spot any differences in financials as well as would be liable should they be found fraudulent.

**FINANCE:**Employment theft policies can be purchased to protect the business against theft but one must be aware of policy provisions relating to the length of time the theft has been going on. Coverage can be limited by time and by policy face amount.

**ASSUME:**Review risk management systems around crime and fraud exposures in the business and calculate the amount not already addressed. Understand this exposure to the balance sheet.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Inability to Access Funds while crime is being investigated.
* 80% of workplace crime is carried out by employees
* One in every four employees has either committed or witnessed workplace fraud
* One in every four employees committing workplace crime has been with their company for more than 10 years
* Only one in three of those who have witnessed workplace crime bother to report it

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Fraud and abuse costs U.S. businesses more than $400 billion annually
* Fraud and abuse costs employers an average of $9 a day per employee
* The Association of Certified Fraud Examiners (ACFE) study reported that the median loss caused by occupational fraud was $159,000

**SOLUTIONS:**

* External audits can be an effective anti-fraud measure for businesses. External audits are the most common anti-fraud measure utilized by businesses and account for nearly half of the cases of fraud detection. Internal audits or controls or even internal fraud examination departments are highly recommended for small businesses. The ACFE study found that only 19.2% of small businesses had internal audit departments.
* Segregation of duties is a type of internal control that can prevent many instances of fraud by limiting the opportunities for dishonest employees to engage in check tampering or billing schemes. If possible, the manager or officer of the organization who will review, authorize and sign checks on behalf of the organization should not be the same person requesting the payment. Similarly, the person who is responsible for receiving and recording payments to the company should not be the same person with the authority to assign payments to customer accounts and make write-offs of delinquent or uncollectible accounts.
* Fraud reporting or hotline programs can be a significant deterrent and prevention measure against fraudulent activities. In fact, “tips” account for the second most frequent detection of fraudulent activity in small businesses, second only to accidental discovery.
* Fraud awareness and ethics training should be provided to employees and managers of a small business. An organization will reduce the fraud-related risk by alerting managers to the types of fraudulent schemes utilized by dishonest employees and informing employees of their duties to report questionable activity.

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* What is your current system to identify employee theft in the workplace?
* When was the last time you had an outside audit performed?
* How do you monitor funds coming in and going out?
* When was the last employee training on theft in the workplace?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <https://www.cnapro.com/pdf/EmplDishonesty%20-%20WolffSamson_1-23-07.pdf>
* <http://www.infographicsshowcase.com/employee-theft-statistics-infographic/>

**Brand Management**

**STRATEGIC RISK –**The mismanagement or failure to address a company's brand can have long-term financial consequences due to loss of market share to competitors and reduced loyalty of current clients.

**BUSINESS RISK –**Brand can be damaged overnight if an organization isn't proactively addressing and a rapid reputation loss would be a detriment to day-to-day operations.

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** A negative brand can impact sales, marketing efficiency, employee morale, attracting and keeping talent. Develop and adhere to a brand management strategy that will reassure customers, prospects, suppliers, and current/future employees.

**MITIGATE:** In the event of a negative incident impacting your brand, develop a response (potentially using a public relations firm as in Reputational Risk) and communicate your response along all forms of your marketing vehicles – website, blog, twitter, facebook, linkedin, television, radio, newspapers, magazines, specialty publications, etc.

**TRANSFER:**Hire outside consultant to manage brand and assume some liability in the event of poor brand management.

**FINANCE:** Micro-captive setup to respond to decrease in sales in the event of brand (reputational) damage.

**ASSUME:** Reputations Corporation, a Vancouver-based consultancy group, reports that 72% of consumers say reputation influences their buying decisions; 80% of employees will accept less pay to work with a company with an excellent reputation; while another 89% say that reputation is a tiebreaker between equal products.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Others in the marketplace define who you are
* Your operation working at peak efficiency because employees do not understand the brand of the business
* Creates confusion in the marketplace
* Failure to win business because people have a negative opinion of you

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Lost opportunity of client now knowing you or not wanting to do business with you because of a negative brand.
* Lack of customer service and productivity because employees not knowing what they are supposed to live up to or do to manage brand.

**SOLUTIONS:**

* Brand management plan (identification of brand followed by an internal/external communication strategy)

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* How are you currently managing your brand within and outside your company?
* What do you believe people in your marketplace think/feel about you?
* What are the clear, powerful thoughts people think about when they hear your name?
* How are you protecting your brand?
* What is the one thing you would change about your brand in the marketplace? Or misconception internally/externally.

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.therightgroup.com.au/our-expertise/organisational-branding>

## Cohesive Management Team

**STRATEGIC RISK –**An organization that fails to build a management team that effectively leads an organization forward, risks the financial well-being of the company in the future due to the lack of implementation of new ideas and the stagnation of the company.

**BUSINESS RISK –**A management team that is not moving in the same direction prohibits growth and slows productivity of the workforce due to lack of direction.

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Build a cohesive management team that trusts one another, engages in constructive conflict, commits to group decisions and holds one another accountable.

**MITIGATE:** Have a strong central leader who understands the principles and benefits of a cohesive management team. This person must reserve the right to object to the direction of a meeting and ultimately will make the final decision that the group must abide by upon everyone’s voices being heard.

**TRANSFER:**

**FINANCE:** D&O policy should the group become dysfunctional and fails to lead the organization resulting in a suit against the group.

**ASSUME:**Understand the cost of having a management team that is not together in the mission of the organization. Loss of sales, failure to attract and retain key production/service talent, loss of productivity, etc.. Determine cost to the organization and either fund for such losses or do nothing.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Inefficiencies among those on the management team
* Inability to push one another leads to lack of conversation and missing new ideas.
* Lack of trust on team can lead to micromanaging and inefficiencies and team second guesses one another.
* Decisions are not supported and are therefore sabotaged.
* Good decisions and strategies never get implemented.

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Lack of implementation of new ideas = $100,000+
* Loss of productivity at the management team level = $10,000+ (Depending on function of team)
* Loss of productivity because of lack of direction = 30-40% of total payroll
* Low level of implementation and eventual stagnation of company = Consolidation

**SOLUTIONS:**

* Read Patrick Lencioni’s book, *The Four Obsessions of an Extraordinary Executive*
* Read Steven M.R. Covey’s book, *The Speed of Trust*
* Build a Cohesive Management Team – The Table Group Solution
* Speed of Trust Workshop
* Hire outside consultant to help build a cohesive team

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* Describe your management teams approach to implementation and execution around strategies?
* What culture do you cultivate among your management team?
* Tell me about the cohesiveness of your management team?
* Are people on the team able to disagree and challenge the team without retribution?
* How does your management team support a decision that they are not completely in favor of implementing?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* Speedoftrust.com
* Thetablegroup.com

**Employee Engagement**

**STRATEGIC RISK –**If employee engagement or employee morale remains consistently low, the ability to attract and retain a quality workforce is greatly diminished and impacts the viability of the organization in the future.

**BUSINESS RISK –**Employee engagement is seen as a business risk due to the daily operations being impacted by not knowing the effective use of payroll.

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Through regular employee surveys, monitor your company’s employee engagement percentages. Establish clear communication channels from the top of the organization to the bottom in the chain of command where ideas are implemented and feedback is acted upon. Effective employee recognition systems are implemented to highlight an accountability culture where employees engage because they understand the sense of purpose and common goals of the organization. Planning and purposeful action will help prevent low morale and negatively impact engagement.

**MITIGATE:** If our engagement numbers are low, we can lessen the severity by having an open dialogue around the numbers in a company-wide communication and begin taking action steps to make an impact on future readings. Review prevention strategies.

**TRANSFER:**

**FINANCE:**Set aside capital for incentive programs within the company to show commitment to increasing engagement. A micro-captive can be used to fund for a loss of customers due to low engagement but not has not been established to date for employee engagement by itself.

**ASSUME:** According to a Gallop study, the average company has an employee engagement rate of 63%. This means for every $1 million in payroll that is being spent, $370,000 is not being used effectively. Calculate these costs and understand the impact this is having on your company’s bottom line.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Productivity
* Personnel turnover
* Low morale
* Toxic environment
* Loss of customers, new hires and new clients
* Loss of team feeling
* Accountability is subverted
* Results suffer
* Loss of or lowered profitability
* Lack of innovation

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Productivity Loss = $700,000 lost on $2 million payroll
* Bad Hire/New Hire = National average of $8,500 each time position turns over. Could be higher or lower depending on industry type & expertise of position.
* Loss of customer = Average revenue per customer

**SOLUTIONS:**

* Employee Engagement Survey
* One or Two Simple Solutions – low hanging fruit
* Performance Management
* Communication Strategies
* Understand Key Performance Indicators – How Measured
* Incentive Performance

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* How much profit do you lose for the lack of productivity?
* Are you reaching your goals in your business?
* What is the next step?
* If you’re not reaching them, what is holding you back?
* What has happened with turnover in the last year?
* Who handles your HR?
* When was the last time you did an Employee Engagement survey?
* What did you learn from it?
* What types of non-productive activities do you see in your office?
* What is your accountability structure?
* Educate on Gallup.
* How many employees feel like this is their company?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* Gallup – http://www.gallup.com/poll/150383/majority-american-workers-not-engaged-jobs.aspx
* Hiring Costs

**EXAMPLES OF SOLUTIONS**

* Worked with a publication company that had never tested their employee engagement and found out through employee surveys that there were a lot of items that the employees wanted to see change in the organization that would help them be more productive and feel like part of the team. They measured 76% of their employees were engaged in the business while 24% were not engaged. This organization had a $6 million payroll which amounted to a cost of approximately $1,440,000 of their payroll was not engaged in moving the business forward. These changes were listened to by management and some of the requested changes were implemented over a calendar year. The following year's results were substantially improved indicating 84% of employees actively engaged in the business. This amounted to a $480,000 improved effective use of payroll.

**Mergers & Acquisitions**

**STRATEGIC RISK –**Impacts the financial future of the organization due to the success or failure of a merger/acquisition can have a long term effect on profitability.

**BUSINESS RISK – Not Applicable**

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Examine factors outside of the financial makeup of a merger such as cultural issues. According to a Watson-Wyatt Worldwide Study, “organizational culture and dynamics of change” was the number one reason for M&A failure. Look at leadership, strategy, current clients (and satisfaction), their external marketing, internal marketing, operations, automation, top sales people, and other behaviors that could potentially cause dissatisfaction with clients or employees.

**MITIGATE:** Prepare contract with a look-back period for areas of concern so that a deal can be undone before it causes further damage to your brand or reputation. Have a good public relations message to help convey to the marketplace the reasons why the merger took place and how it benefits them.

**TRANSFER: Not Applicable**

**FINANCE:** D&O policy for liability if merger/acquisition performs poorly and investors or employees file suit. 831(b) micro-captive established for risk of revenue loss in the event of an underperforming merger.

**ASSUME:** According to the Wall Street Journal, Forbes & Fortune Magazine, 70% of M&A deals fail to achieve the anticipated synergies; 50% report an overall drop in productivity in the first 4-8 months, 47% of acquired company executives leave in the first year with 75% leaving within the first three years; 23% of acquisitions earn their internal rate of return; 58% of mergers fail to create substantial returns to shareholders; the average executive grade the financial performance of their acquisitions as a “C minus”.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Clarity around environment
* HR impact
* Culture issues
* Risk analysis
* Coverage analysis
* Software capabilities
* Overpayment of acquisition
* Failure to think through the operational issues creates redundancies and inefficiencies
* 83% of all M&A failed to produce any benefit to stakeholders

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Culture Issues = $50,000++
* Coverage Analysis = $10,000
* Decreased productivity due to lack of culture blending = $100,000+
* Job losses, and the attendant uncertainty, anxiety and resentment among employees at all levels may demoralize the workforce to such an extent that a firm's productivity could drop between 25 to 50 percent.

**SOLUTIONS:**

* InCite Culture Assessment Tool
* Coverage & Risk Analysis on company to be acquired
* Comparison of HR policies & procedures

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* Are you considering mergers or acquisitions in the future?
* Have you considered corporate history on both sides of mergers?
* How do you analyze the cultures of future M&A targets?
* Have you considered the reasons for success of future M&A and how they may or may not be a fit for your organization?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* [http://EzineArticles.com/3685280](http://ezinearticles.com/3685280)
* Book: Reasons for frequent failure in Mergers and Acquisitions: A comprehensive analysis (Thomas Straub, 2007)
* <http://itapintl.com/facultyandresources/articlelibrarymain/the-impact-of-culture-on-mergers-a-acquisitions.html>

**Succession & Perpetuation**

**STRATEGIC RISK –**A strategic risk due to the impact it has on current and future evaluation of the company.  It could also have an impact on the ability to stay in business due to a catastrophic loss (key employee or owner).

**BUSINESS RISK – Not Applicable**

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** The best time to prepare for the perpetuation of your business is the day you open your doors. Begin the process by identifying potential candidates either outside of your business or inside your current employee population. Once candidates are identified, put a strategy in place to create a perpetuation plan within twelve months, including leadership training for the candidates as well as financial plans in place to ensure that the appropriate financing needs can be obtained. Identify business systems, infrastructure, performance management, human capital & leadership buy-in to move this process forward. Engage an attorney that specializes in perpetuation and succession planning.

**MITIGATE:** In the event of an unforeseen need for immediate perpetuation, establish financing triggers that can put immediate funding in the business (i.e. life insurance) to purchase shares of deceased or removed partner. Establish clear communication plan to employees and community proactively addressing concerns that may arise.

**TRANSFER:**Have contract in place with local competitor to purchase majority stake or entire business in the event of retirement or death. Can also sell out to competitor today to transfer this risk immediately.

**FINANCE:** Establishing life insurance policies on each stake holder with a well-funded buy-sell agreement in the event of death or retirement.

**ASSUME:** Understand the cost associated with not preparing such as business not continuing in the event of the owner’s death or retirement, business less attractive to key talent, lower employee morale & decreased productivity.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Lack of a plan prevents the business from continuing on in the future
* Lack of a plan also diminishes the value of the organization in the marketplace
* Creates leadership gap when it’s time to transition the business
* Loss of potential clients due to uncertainty of doing business with a company with no plan in place
* If done last minute, creates chaos within the organization

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Impacts the value of business when sold from 10-40%
* Only 1.5% of companies survive into the 3rd generation of management
* Loss of potential customers by average size customer multiplied by those lost
* Only 40% of American businesses have a succession plan in place
* 55% of the nation’s CEO’s scheduled to retire in the next 3-4 years have not yet named a replacement

**SOLUTIONS:**

* Begin discussions around potential candidates for the future and put strategy in place to create a plan in 12 months.
* Identify business systems, infrastructure, performance management, human capital & leadership and obtain stakeholder engagement to move the process forward.
* Engage attorney and CPA (CA in Canada) specializing in perpetuation planning.
* Fund the plan.
* Develop future leaders through training programs to support their future leadership.

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* Share with me your formal perpetuation plan and your date of execution?
* What processes are in place today to develop future leadership perpetuation of the organization?
* Who has been identified internally to be the perpetuation of you company?
* If something happened to you today, what plan is in place to seamlessly transition ownership & leadership?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://smallbusiness.chron.com/business-perpetuation-plan-784.html>
* <http://archive.sba.gov/idc/groups/public/documents/sba_homepage/serv_pubs_eb_pdf_eb1.pdf>

**EXAMPLES OF SOLUTIONS:**

* Problem: Client was transitioning ownership over a three year period to an outside party and being taxed at the highest level for the transaction.
* Solution: We worked with the client to restructure the buyout in a more tax favorable manner.
* Result: This saved the incoming owner over $1,000,000 in taxes over the three year period which allowed them to accelerate the pay-off.
* Bottom Line Impact: $1,000,000 over three years

**HR Record Management**

**STRATEGIC RISK – Not Applicable**

**BUSINESS RISK –**Failure to maintain accurate and secure HR records can slow down the organization from hiring to termination, and can create a large monetary loss due to governmental fines or lawsuits from employees if records lost.

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Develop systems around how your organization will retain, store and access employee files in the future as business continues to go paperless. Companies must remain aware of the legal requirements for record-keeping relating to different areas of their operations.

**MITIGATE:** In the event of a loss, various recovery contractors are in business to recover lost files. Much like a data breach, a response plan should be generated immediately alerting any current or former employee of a lost or compromised record.

**TRANSFER:**Cloud-based software systems exist that allow companies to store confidential HR documentation off-site, with little risk to the employer.

**FINANCE:**Cyber liability can cover a data breach and some policies can respond to data recovery losses.

**ASSUME:**Understand the HIPPA and other regulatory fines associated with not keeping appropriate HR records and financially prepare.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Potential employee lawsuits
* Filing 5500 on self funded plans – disclosure
* Medicare part D notification
* Data protection
* FMLA issues

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* HIPAA – personal issue – employer PHI info passed in office = $100 to $25,000 per violation
* 5500s penalties (disqualify plan) = $50,000 per disqualified discrimination
* FMLA Issues

**SOLUTIONS:**

* Secured email solution
* Affiliations with CPAs
* Check List (compliance) Annual check
* Healthcare Navigator Tool™
* Actuary and compliance check systems

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* What kind of policy and procedures are in place today in these areas?
* How are you preparing for these issues as they proceed?
* What were the results of your last data security audit?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/penalties.html>
* Most frequent data loss is from stolen or accessed electronics and paper files walking away vs purposeful theft

**Intellectual Capital**

**STRATEGIC RISK –**Strategic risk due to the potential for financial impact in the future of the organization.

**BUSINESS RISK – Not Applicable**

**HAZARD RISK – Not Applicable**

**Methods to Manage this Risk**

**PREVENT:** Prior to employment beginning, require in writing exclusive ownership of all intellectual property created by employees. Exit interviews for an acknowledgement that the employee understands they are not leaving with company assets and will not be disclosing trade secrets. Confirm everything in writing to the new employer. Update electronic use policies to make sure that all files taken offsite be password protected or encrypted. Monitor employee blogs for references to your company and you have the right to react to inappropriate postings. Use confidentiality agreements when outsourcing. Monitor trademark use on the internet (to maintain trademarks, court say that the owner must police them and point out inappropriate use). Require employees to encrypt their home wireless networks. Trademark intellectual capital, if possible.at could cause damage.

**MITIGATE:** In the event of piracy of intellectual capital, have an established relationship and regular dialogue with legal counsel. Respond quickly and ferociously to not only protect the capital but also your reputation of defending it vehemently.

**TRANSFER:**Create relationship with outside consultant who generates all intellectual capital, updates trademarks, and monitors then gives you exclusive rights to that intellectual capital.

**FINANCE:** Purchase patent insurance through Lloyd’s or set up 831(b) micro-captive to respond in the event of infringement.

**ASSUME:**Quantify the cost of your largest competitor gaining access to your intellectual capital. Plan accordingly.

**ADDITIONAL RISK INFORMATION AND FACTS**

**PROBLEMS IDENTIFIED WITH THIS RISK:**

* Former employee steals ideas or trade secrets and gives them to competitor
* Competitor begins using your marketing strategies to attract clients
* Someone from outside your marketplace is using your information on their website.
* Someone has rebranded your white paper as their own.

**QUANTIFY CURRENT AND POTENTIAL COSTS:**

* Potential loss of client if competitor steals trade secrets = Average revenue per client multiplied by the number of clients you would lose.
* Dollars spent creating intellectual capital now wasted = hours spent in development multiplied by wage per hour

**SOLUTIONS:**

* Prior to employment beginning, require in writing exclusive ownership of all intellectual property created by employees. Exit interviews for an acknowledgement that the employee understands they are not leaving with company assets and will not be disclosing trade secrets. Confirm everything in writing to the new employer. Update electronic use policies to make sure that all files taken offsite be password protected or encrypted. Monitor employee blogs for references to your company and you have the right to react to inappropriate postings. Use confidentiality agreements when outsourcing. Monitor trademark use on the internet (to maintain trademarks, court say that the owner must police them and point out inappropriate use). Require employees to encrypt their home wireless networks. Trademark intellectual capital, if possible.

**QUESTIONS TO ASK TO IDENTIFY NEED:**

* How are you currently protecting your intellectual capital?
* What would it cost you if your best employee took your trade secrets and handed them to your competitor?
* What is your average revenue per client?
* How much time and money do you spend each year creating differentiators between you and your competition?

**FACTS AND RESEARCH TO UNDERSTAND THE RISK:**

* <https://sites.google.com/site/wisdomcapture/organizational-innovation/management-of-intellectual-capital/intellectual-capital-protection-paper>
* <http://en.wikipedia.org/wiki/Intellectual_capital>