*Integrated Risk Management Solutions, LLC*

James E. Blair, President

December, 2017

Dear Colleague;

## Human Behavior is the Risk of the Day!

While hurricanes, earthquakes and wild fires are consuming personal, business, government and insurance dollars by the billons in 2017, closely followed by the billions expended on cyber-breaches, Human Behavior is capturing the headlines. And, more importantly it is impacting the lives of workers, business leaders and the public. There are more than enough material risks from uncontrollable risks to occupy the Risk Agenda.

BUT, unacceptable Human Behavior is upstaging it all.

Most captivating are the reports of Sexual Harassment and misconduct in virtually every business sector and many governmental entities in the country. Compounded by business miss-treatment of customers and employees by Wells Fargo, pricing and employee manipulation by Uber, sexual harassment by public figures at FOX and NBC, and intentional misstatements regarding cyber-breaches at Yahoo and Equifax, public confidence in businesses is a major risk to be mitigated through proactive communications, strengthened Risk-based governance and a return to strong Ethical Behavior.

So, what is this notion of Ethical Behavior? Leaders are expected to produce business strategy, sales and consumer services, operational excellence and nimble adjustments to business conditions that produce results to satisfy shareholders and stakeholders. Hundreds of books are written about Ethics and Leadership, but simply said: leaders achieve success through 1) clear and rhythmic communications to all stakeholders, 2) a risk based strategy that anticipates disruptions, 3) alignment of all parts of the organization toward common goals, 4) regular measurement of progress and the passion to adjust when unexpected risks arise and 5) recognition of success. It is imperative that these steps are conducted within a culture of honesty, trust, integrity, passionate assessment of progress, nimble adjustment to circumstances, and operational excellence.

The establishment of an Ethical Culture is the duty of the Board, owners and the C-leaders of the organization. Now the concept is easy to talk about, but putting it into action is another matter. Given the demand for an Ethical Organization, top leaders/Board must establish a governance process that 1) establishes expectations, 2) communicates the "tone" and 3) rhythmically measures the pulse and performance. Use of internal and external measurement systems is critical to a Board committee focused on Risk, Ethics and Culture. In 2018, sixty percent of Boards are expected to increase attention to CEO succession (NACD report 12/1/17) – this portends increased attention to leadership, organizational culture and Ethical Behavior! Top-level governance processes that focus on the Human Behavior of organizational leaders is the Risk Management solution.

P.O. Box 334 Littleton, CO 80160-0034 jeblair@integratedrisksolutions.com
303-795-9754 (O) 303-734-1814 (F) 303-886-8450 (C)
www.integratedrisksolutions.com



Your organization, like many others, works hard to operate successfully and present an honest product/service that customers can rely upon. It's a big job, and is most effectively supported by Ethics, a culture of trust and effective management of Risk. Remember "we take risk to generate cash – we spend cash when risk is not managed".

**Risk = Cash!**

Effective management of Risk is every business leader's and member's responsibility. Certainly, organizational culture is established by top management and the Board. Unfortunately, responsibility is often schlepped off to HR or the Compensation Committee. An urgent change is needed that can be achieved by top-level Risk Governance practiced by a Risk Management Executive Council (RMEC). Tackling the Risk of Human Behavior as a material and urgent imperative. A creative example is Fox's establishment of a Board level Workplace Culture Panel to oversee the internal h Human Behavior of the organization – a very positive action!

This Quarterly Advisory would be incomplete if we didn't discuss the facts regarding magnitude of disaster risk and the evolving risks of cyber. This year more than $370 billion in global physical damage has been caused by unexpected events of nature ($200+billion in the US). These numbers understate the costs of business disruptions, revenue loss and human costs – the numbers could easily be double. We simply cannot avoid a hurricane, and FEMA has reported "they are out of bandwidth" to deal with more damage. Effective Risk Management is the anticipation of disruptions and proactive preparedness to Recognize, Respond and Recover – businesses will need to move toward independent self-reliance.

Cyber incidents remain out of control. The bad guys continue to stay ahead in the race to steal, manipulate, kidnap and sell private information on the web. The numbers we've stated in previous Advisories continue to grow and organizations are slowl to disclose the costs of cyber breaches. Equifax has spent nearly $100MM on repair and recovery from the breach of more than 160 million records, including 250,000 Social Security numbers (see attached 14 steps required for recovery). This lost data will resurface in the dark web for decades, forcing citizens toward a higher level of Risk awareness for a lifetime. These Risks are manageable under the stewardship of a top-level Risk Management Governance process (the RMEC).

*Integrated Risk Management Solutions* provides Advisory services to help strengthen your business. I look forward to your thoughts and questions – please contact us.

Manage Your Risks Well,

Attachment

***Risk Management is Every Team Member's Business***

P.O. Box 334 Littleton, CO 80160-0034 jeblair@integratedrisksolutions.com
303-795-9754 (O) 303-734-1814 (F) 303-886-8450 (C)
www.integratedrisksolutions.com

# Managing Risk = Cash Flow

Typical returns are 4:1 ROI and significant cash flow improvement

Risk is anything that impacts cash flow! Successful companies manage risk more effectively than competitors. By practicing a "Risk Awareness" culture that engages every level of the business in prevention-centric behavior, cash flow is improved.

Key Risk Management Facts:

- Companies spend between 7 - 10% of revenue on risk-related costs, including:
  - Safety - Security - Information Security - Health & Wellness
  - Absence* - Theft - Fraud Prevention - Revenue Inefficiency
  - Audit - Compliance - Investigations - Settlements
  - Claims - Insurance - Crisis Management - Emergency Response

  * Incidental absence can increase the costs of employee health and wellness programs by 2X.

- Risk costs are incurred in multiple corporate silos hiding the "Total Cost of Risk."
- 75% of company information system risks come from employees and trusted vendors.
- FM Global, a world-wide property insurance and engineering firm, recently estimated that company earnings volatility can be reduced by 50% through effective Risk Management prevention and preparedness programs.
- In 2016, companies that manage risks effectively will receive the best insurance prices and maximize the option to *self-insure*.
- Enterprise-wide Risk Management is a complete vision of company risk. A strong Risk Management culture helps a company respond well to unforeseeable events.
- Documented and tested Business Interruption/Scenario Plans sustain key operations during an emergency and improve company survival by 70%.
- Uncertainty and financial pressure renew the need to manage risk. These pressures have always been present, but the magnitude and visibility is at an all-time high.
- Third party vendor transactions often result in 10% or greater errors and inaccurate billing.
- Sarbanes-Oxley, Dodd-Frank and compliance audits only test transactional controls – operational controls are "the source" of risk – **Operations Assurance is the key!**
- Regular Operations Assurance reviews can improve revenue efficiency by up to 20%.
- Synergy from a holistic focus on risk, cost/revenue efficiency, loss reduction, underperforming vendors and fraud produce impactful cash flow improvement.

**2017 Global Risks Defined by:**

**World Economic Forum**

- Extreme weather events
- Water crisis
- Natural disasters
- Failure of climate-change mitigation & adaptation
- Large scale involuntary migration
- Terrorist attacks
- Interstate conflict
- Un/under employment
- Cyber attacks
- Man-made environment disasters

**Executive Opinion Survey***

- Un/under employment
- Energy price shock
- Fiscal crisis
- Failure of national governance
- Profound social instability
- Failure of financial mechanisms
- Terrorist attacks
- Failure of critical infrastructures
- Asset bubble
- Cyber attacks

* WEO Survey 2017

***Manage Your Risks Well!***

P.O. Box 334
Littleton, CO 80160-0034
jeblair@integratedrisksolutions.com
303-795-9754 (O)
303-734-1814 (F)
303-886-8450 (C)
www.integratedrisksolutions.com

# 14 Steps Required to Respond to a Breach

With everything invested in the health and resiliency of your information systems, preparations should be made for the day you must respond to an information breach. These preparations and plans should be under the stewardship of a Risk Management Governance Council which we have presented in most Client Advisories from *Integrated Risk Management Solutions, LLC*.

Please consider all 14 response action steps:

1. Breach Detection – Application level detection is critical to detect within hours.
2. Forensic Analysis – What, where, by whom, and who is impacted - 1-3 days.
3. Repair – The level of damage and the fixes needed to get back online within your Business Interruption Plan – 2-4 days.
4. Identification of Parties affected – Customers, vendors, employees, shareholders; – 5-10 days.
5. Legal Protection – Establish an Attorney-Client Privilege protocol to protect the details of your investigation and action steps (anticipates longer-term litigation).
6. Communications Plan – Pre-prepared communications for internal and external stakeholders – 1-3 days.
7. Notify Regulators – 48 States require notification of the Attorney General and the affected parties within a "reasonable" period – 30-45 days.
8. Notify Parties – Initiate a paper mailing notification of affected parties. Establish an 800# call center to respond to inquiries. This process took 12 months for the U.S. Office of Personnel Management breach (24 million individuals).
9. Credit Monitoring – Offer services to affected parties as a matter of client relations.
10. Identity Repair – Offer services to affected parties as a matter of client relations.
11. PCI Analysis and Repair of Systems – The Credit Card providers oversee your credit card processing and will expect thorough reports of the findings in item 2 and 3. Expect heavy fines and penalties.
12. Regulatory Examination and Fines – Prepare with legal counsel for fairly heavy handed regulatory penalties.
13. Litigation – Insurers are hesitant to write many cyber-policies because of the unknown and lengthy "tail" liabilities that will accrue over 5-10 years.
14. Reputation Recovery – Your organization's name will be on the news and internet. You can't hide from an information breach. Reputation Recovery starts with the Communications Plan listed in item 6. Chipotle is spending $100 million or more to recover their brand reputation following the health scare from E. Coli.

The damage from information breaches is serious. Ponemon estimates the cost per record breached (to pay for the 14 steps) is now $201, and average total cost per incident at $5.85 million. On the other hand, Risk Management is not expensive! The Governance process amplifies "Native Organizational Intelligence" in a manner that strengthens the business and its constituents.

*Integrated Risk Management Solutions* provides Advisory services to help strengthen your business. I look forward to your thoughts and questions – please contact us.

***Manage Your Risks Well!***

P.O. Box 334 Littleton, CO 80160-0034 jeblair@integratedrisksolutions.com
303-795-9754 (O) 303-734-1814 (F) 303-886-8450 (C)
www.integratedrisksolutions.com