



James E. Blair, President

June 2023

Dear Colleague:

It is the Magnitude and Frequency!

The January forecasts of global risks presented in Davos, Switzerland were quite accurate. Business Interruption, Cyber, Geopolitical, Climate Change, Natural Disasters, Inflation, Energy Uncertainty and People! All have impacted your business in the last 6 months challenging the very best in business and governmental leaders. So, these risk factors have been with us forever. What is new is the enormity of the damages and costs, and the number of people negatively impacted. More incredible is that these factors show up in a compounding fashion – we don't get one without another. The common impact is Business Interruption! If every reader of this Colleague letter took two steps toward a practiced Business Interruption Plan (BIP) the economy and industry would be far more secure and resilient during the next year. The cost is minimal!

Simply, we can agree that bad things happen every day and in every business. The factor that distinguishes successful businesses from the “also-rans” is the speed of response and recovery. A well-crafted BIP prepares your team members to be more alert to risk prospects, engages their thinking in alternative approaches to operations, collaborates across organizational structures and prepares for the moment when an interruption occurs. The team is prepared for any event and collaborates in an integrated fashion during an incident – no matter the size. Customers and suppliers learn to rely on your services and the can-do attitude of the team. A well-prepared team walks with a confidence that others don't. Customer disruption is minimized, and recovery costs are reduced. The payback is infinite! And you gain a customer for life.

The costs are Minimal

Two primary examples of effective BIPs have been presented this year. When Russia began threatening the energy supply chains in Europe and NATO countries instant collaboration began to assess alternatives and creative solutions to sustain supplies through the winter months, to leader's credit. We did not see the friction often accompanying cross-border situations. Rather, adjacent countries immediately initiated creative approaches to supply chain and alternative energy sources of wind, solar, natural gas, and Liquefied Natural Gas. Even the disruption of the Nord Stream 1 pipeline did not cause insurmountable public distress. Business Interruption actions across country boundaries integrated to find creative solutions and alternative processes. Should we expect that some well-practiced prevention system was already in place? Likely not!

A real-time incident occurred on June 11 when the I-95 freeway overpass collapsed in Philadelphia. A 100' long by 100' wide section of the freeway collapsed unexpectedly disrupting the travel of 160,000 vehicles daily that carry much of the commerce in the Northeast. Normal recovery and reconstruction would consume 9-18 months.



Page 2

However, the Governor gathered a cross-organization team to find alternatives to the lengthy steel and concrete replacement. Creativity appears to rule, and the cavity caused by the overpass collapse will be filled by 2,000 tons of crushed recycled glass pebbles, compacted, and then paved. The goal is 2 weeks – I’m anxious to watch this unique approach to an otherwise very time-consuming operation. The long-term permanent fix can take the normal course.

What is common between these two examples? First is the magnitude of the incidents. Both have the potential to cause enormous economic and human damage. The time for recovery was urgent and creative recovery methods were demanded. Strong collaborative leadership was required and both projects received that attention. While the results will ultimately be costly in terms of physical reconstruction, the costs from freezing temperatures in Europe and disrupted economic prosperity in the Northeast were minimized thanks to creative engineering and deployment.

And Cyber!

Cyber-attacks deliver threats we have yet to completely comprehend. During the past two years more than \$7 billion in new venture investment dollars have been committed to cyber protection. Understand that the bad guys have likely committed a similar amount - \$14 billion in total. As creative protection schemes are developed and deployed, cyber attackers are creating new avenues into your information systems. This month alone, cyber-attacks have crippled the Driver’s License bureaus in the States of Louisiana and Oregon. Additionally, numerous large hospital and educational centers, the Federal Department of Energy and other unnamed agencies, British Airways and the British Broadcasting Corp. have had their file systems hacked through a software package called MoveIT. The entry tool used by Russian hackers was Business Email which simply delivers an attachment. NOTE – coach all employees not to click on any email attachment they don’t recognize or expect.

The good news is that Ransomware attacks have dropped in the US. Not so for Europe, but data reflects progress. Now, as the volume has shrunk, the ransom demands have skyrocketed to an average of \$360,000 each. Smaller companies are the primary targets, paying ransom in the range of \$200,000 each. Insurance often covers only a small portion. The Business Interruption lesson is “early detection” which your employees will be the first to know.

These are the Risk Management principles foundational to the work of *Integrated Risk Management Solutions, LLC*. We help you prepare and deliver trusted and responsive products/services. I look forward to your thoughts and questions – please contact us.

Manage Your Risks Well,

Attachment

Risk Management is Every Team Member’s Business



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 in multiple silos hiding the “Total Cost of Risk” and measurable ROI.
- 80% of company information system risks come from employees and trusted vendors.
- FM Global, a world-wide property insurance and engineering firm, estimates that company earnings volatility can be reduced by 50% through effective Risk Management prevention and preparedness programs.
- 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 more nimbly respond 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.

2023 Global Risks Defined by:

World Economic Forum

- Cost of living crisis
- Natural disasters/extreme weather
- Geoeconomic confrontation
- Failure to mitigate climate change
- Erosion of social cohesion & societal polarization
- Large environmental incidents
- Failure climate change adaptation
- Cybercrime & cyber insecurity
- Natural resource crisis
- Large-scale involuntary migration

Executive Opinion Survey*

- Business Interruption
- Cyber Incidents
- Ukraine Conflict & Geopolitical tension
- Failure of Digital Supply Chains
- Microeconomic concerns
- Energy crisis
- Regulatory changes
- Natural catastrophes
- Climate Change
- Shortage of skilled labor
- * Protiviti -ERM Initiative

Manage Your Risks Well!

January 2023