



James E. Blair, President

June 2021

Dear Colleague

Resilience and Reliability!

The first 5 months of 2021 have presented risks beyond those of 2020. While recovery from the COVID-19 disaster has been steady and somewhat predictable, global disruption to operations, inventories, and supply chains have slowed the pace of what otherwise could be a most robust and reliable economic growth trend. While the global GDP is forecast to grow in excess of 5%, no one can predict a level of stability and reliability. We enter a new phase of the imperatives for effective Risk Governance that anticipates and prepares to Respond and Recover from the unknown.

To date we have witnessed supply disruptions from the grounding of the ship “Ever Given” in the Suez Canal resulting in an estimated “daily” \$10 billion impact on the global economy. Supplies have been delayed since March 23, and many days after the ship was refloated on March 29. The math is wild – assume 60 days at \$10 billion/day. And from just ONE ship! Can we assume the Canal Authority and/or ship owner had a business interruption plan in place?

Other major operations components are in short supply including computer-chips, fuel, steel, water, skilled workers, and laborers to meet market demands associated with the economic recovery from the year of COVID-19. It appears that few anticipated the sling-shot pace of recovery from the economic suppression of the disease year. Globally we got caught flat-footed twice; first, not anticipating the disruption from the pandemic and second, missing the signals that recovery would challenge the entire supply chain to prepare for new demand.

About the only thing that is not in short supply is cyber and information breaches. Ransomware attacks are up 150% delivering more than \$350 million in profits to global bad guys. Businesses like yours are disrupted an average of 21 days and then anticipate an average 287 days to fully recover. The average payment of ransom is \$312,500 and the overall cost of an attack is about \$4.4 million. Who has that level of reserve to cover the costs, much less the lost revenue, reputation and production? Cyber breaches and Ransomware are the most frequent and expensive risks to business operations (more so than natural disasters like floods, tornados and hurricanes).

Insurance costs have skyrocketed this year with premium increases in the 30-50% range. Some liability policies have increased 2-3X over previous years. And insurers are not optimistic about a successful year. The tails on cyber breaches are multi-year with costs in the billions. Ransomware alone is expected to cost \$1.4 trillion globally in 2025. Insurers who have denied Business Interruption claims from COVID-19 are increasingly losing the cases. The disease did result in employment disruptions and courts are finding for the claimants. 2021-22 may see a number of insurers fail.

Business Interruption, Resilience and Reliability are the single most important Risks to anticipate and prepare for, no matter the reason or root cause.



The three R's – Recognize, Respond and Recover remain paramount Risk Management principles.

Optimistic Outlook!

It is easy for a Risk Guy to focus on the dark side of operations, and page 1 provides more than enough to dampen the vision of a future. However, remember that we all go into business and take risk that generates cash. When risk is well-managed, operations and economics soar. Effective Risk Governance has never been “more-timely”.

Consider the positives; 1) as vaccinations grow the health and safety of the public is rapidly improving, 2) employment is growing, 3) wages are increasing, 4) global demand is growing, and 5) consumers are spending again. With the addition of stimulus initiatives that appear to be continuing, and with massive investments in infrastructure there is no reason to fear a downturn or disruption. We may all get impatient at the amount of time required to get these initiatives approved and underway, but the next couple of years should be prosperity and growth. The thought of “Build Back Better” is quite likely to happen.

Planning and preparing is our challenge. While much of the optimism relies on Government spending, industry is also sitting on a pile of cash for investment as well. As funds are available strategic and operations plans must be governed through a Risk Management lens that visions the outcome while anticipating what might not go well, including poor planning, training, deployment, cyber-breach, Ransomware, theft, fraud (still about 4% of revenue), uncertain regulations, inflation, political rancor, human talent, skilled workers, fragile supply chains, and foreign influence. All major-league risks that cause Business Interruption.

Design your future with Business Resilience and Reliability in the forefront of everyone's thinking. Engage your entire team in the practice of Integrated and Agile Risk Management. When something goes Awry, Recognize, Respond and Recover. It works!

Top leaders must continue to invest in Cyber Risk Management. As uncomfortable as it might be, embrace Risk Governance of IT based systems and security expertise. Implement 1) Multi-factor authentication, 2) consistent patching, 3) Resilience and Readiness procedures and 4) Reliable and tested back-ups on separate and protected networks. If you don't do this, at least prepare to be Cyber-breached. Be Prepared!

Everything [Integrated Risk Management Solutions, LLC](#) represents is preparing you to 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.

2021 Global Risks Defined by:

World Economic Forum

- Infectious Diseases
- Livelihood crises
- Extreme weather events
- Cybersecurity failure
- Digital inequality
- Prolonged stagnation
- Terrorist attacks
- Youth disillusionment
- Social cohesion erosion
- Human environmental damage

Executive Opinion Survey*

- Pandemic caused regulations
- Economic growth restrictions
- Pandemic caused consumer demand
- Digital skills shortage
- Privacy & Information Security
- Cyber-threats
- Regulations impairing operating resilience
- Succession and top-talent retention
- Resistance to cultural changes
- Competing with digital-born competitors
- * Protiviti & UCSU -ERM Initiative

Manage Your Risks Well!

January 2021