



James E. Blair, President

June 2024

Dear Colleague:

Preparedness and Response!

The variety and magnitude of economic impacting risks experienced during the first 2 quarters of 2024 are nothing short of “mind numbing”. Physical damaging risk incidents have caused \$20 billion in insurable damages and \$45 billion in total economic impacts across the globe. A January 1 earthquake in Japan started the year with immediate damages, followed by severe wind, flood, and fire events across Europe and the U.S. Houston suffered \$7 billion in damage from a Severe Convection Storm (SCS) in May, and during the last 2 weeks Texas, Oklahoma, and Arkansas were hit by tornados and hail leaving more than a million customers without power. Twelve \$1 billion events have occurred globally to-date, with 8 occurring in the US. While human tragedy is unfortunate, the disruption to business and public safety operations widens the loss of operational continuity for millions.

Cyber damaging risk incidents impact everyone. To date Ransomware, Business Email Compromise (BEC), and cyber-theft of sensitive data including financial transactions has caused \$12.5 billion in economic losses. During the first quarter Ransomware attacks are up 429% over the similar period of 2023. Not only are financial losses serious, but the magnitude of breaches is beginning to take an emotional toll on the level of confidence business leaders must face regarding the prospect of damaged deals, loss of privacy, and operational disruptions on a 7x24 basis. It’s reasonable to wonder whether “anything is safe”.

Likely, the most volatile risks are the result of political and geo-political incidents resulting in human threats and war-like global actions. Most concerning are the Russian attacks on Ukraine and the Israeli actions in Gaza and Palestine. Middle eastern nations are certainly willing to join together to disrupt Israel’s peace and war-like attacks on Hamas. The culmination of these actions is supply chain disruption to sea lane shipping, and the confidence of shippers. Prices have skyrocketed 30% in the first 5 months of 2024. Equally disturbing are the supply chain dynamics of Russia/Ukraine. China, Viet Nam, and India are shipping military hardware to Russia – a phenomenon not seen before. Equally the western nations are providing massive shipments into Ukraine expanding threats from the Kremlin of reprisals. All are risks that your teams should be aware of and prepare for.

Recognition, Response, and Recovery

Given the wide array of physical, cyber and political risk you face daily along with the seemingly impossible capability to mitigate some or all, preparedness for any and all risks is the most important action businesses can take. Dedicating resources to Business Interruption Planning is a wise investment. Task a small inter-departmental team to regularly evaluate the risk landscape and consider the resources, communications paths, and approval processes that can be deployed the day bad stuff happens.



Page 2

Anticipate the impact of bad weather events, fires, mass illness, political unrest, supply chain disruption, cyber-attack, privacy disclosure, 3rd party provider disruption, Information Services breach, sales production system failure, Artificial Intelligence dysfunction, reputational challenges including CEO/board misconduct, etc. Establishment of a practiced Business Interruption Process is one of the best investments businesses can make. It prepares you for anything imaginable, and perhaps beyond that. Muscle memory is developed to anticipate risks and operate with confidence that the business can handle it. *Integrated Risk Management Solutions, LLC* specializes in Business Interruption services and is prepared to assist you.

Governance!

Integrated and cross-functional governance is the ultimate key to Risk Management success. The National Institute of Standards and Technology (NIST) and the National Association of Corporate Directors (NACD) have recently released new findings and guidance for effective corporate risk governance. NIST published a new pillar in its 2.0 standard for cyber-breach protection and NACD recently updated its guidance to corporate directors. Both establish the principle of Governance as a key to effective management and response to the array of risks reported in this advisory. You will begin to see emphasis on governance from the SEC, FINRA, the FDIC, and other regulatory agencies. We've discussed quality governance for 12 years and our best clients practice it regularly. The best practice is publicly announced last.

Insurers are noticing as well. Recent reports indicate that major insurers are withholding claims payments to customers who do not practice effective governance, particularly for cyber-breach claims. A word about Artificial Intelligence (AI) – developments in the world of AI are coming daily and organizations must apply the principles of governance and Business Interruption to everything associated with Information Systems. Investment in AI policies and training is critical, along with investment in protective systems that can recognize material generated by Large Language Models (LLM). The time is now.

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 respond more nimbly 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 are 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 produces impactful cash flow improvement.

2024 Global Risks Defined by:

World Economic Forum

- Misinformation & Disinformation
- Extreme weather events
- Societal Polarization
- Cyber Insecurity
- Interstate armed conflict
- Lack of economic opportunity
- Inflation
- Involuntary migration
- Economic downturn
- Pollution

The Conference Board

- Economic downturn/recession
- Inflation
- Global political instability
- Higher borrowing costs
- Labor shortages
- Rapidly advancing AI technology
- Higher labor costs
- ESG backlash
- National debt
- AI Risk Governance

Manage Your Risks Well!

January 2024