Integrated Risk Management Solutions, LLC

James E. Blair, President

September 2023

Dear Colleague:

PolyCrisis is our new Reality!

In these Client Advisories you have read about Compound Risks, Accumulating Risks and Multiple Risks. The year 2023 has coined the word "PolyCrisis" to help leaders comprehend the confusion they might feel in today's risky world with incidents occurring simultaneously and with very little alignment or correlation. The factor of time also feeds PolyCrisis events when a catastrophic weather situation delivers hurricane winds and then enormous rains or ocean waves that bring severe flooding. All are compounded by inadequate preparation of the public at large and potentially greater damage due to insufficient maintenance of infrastructure or response resources.

This year the US has experienced 23 severe weather extreme events with the result of massive damage and cost to communities, your employees and your businesses (to date $58 billion in damage and more than 250 fatalities). Through the first 6 months of the year, approximately $194 billion in total economic costs have been imposed globally by weather related crises, with only $54 billion insured. The storms cannot be controlled, and we are left with the action steps of preparation and response. A nasty taste of risk reality!

The cyber-world is even more costly with every form of cyber-attack increasing over previous years. To date, 33 billion attacks have occurred globally, which is one every 39 seconds. The estimated cost is $8 trillion globally of which a fraction is covered by insurance. The accumulated total cost of catastrophes and cyber is staggering and a severe burden on businesses and governments. Both types of disaster drive the cost of business upward and seriously impair the delivery of products and services. An amazing example of the risks associated with cyber is the Starlink system deployed in support of the Ukrainian fighting forces which at the point of an attack on Russian naval forces was switched OFF! This is a serious and dangerous lesson in inadequate 3rd party risk management.

The Regulators are Here

This summer the SEC adopted new reporting rules for cyber-attacks that may have a material impact on public company operations. Regulated entities must report cyber-related incidents that have a potential material impact within 4 days of recognition. This is a heavy burden on businesses since most cyber-attacks take time to mature into recognizable business disruption. Clorox is the first public company to report, which they did on August 14. Subsequently, the company has made 6 additional reports including in their 3Q 8K filing. Cyber risk is complicated, time consuming and costly.

The better solution is the proactive adoption of cyber risk prevention and response techniques. This is the SEC's goal anyway. Adoption of the risk governance principles offered by *Integrated Risk Management Solutions LLC* is a first step.

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

This seemingly heavy hand by the SEC is unfortunately earned by the business community. Brian Krebs, immediate former Director of the Cyber Intelligence Service Agency (CISA) and now a consultant, reports an analysis of public documents from the Fortune 100 companies that states a strong commitment to cyber and data security. However, reading the fine print, Krebs discovered that industry is not actually backing-up their commitment with top cyber executive talent. The majority of the 100 still list a Human Resources executive as leading the cyber-security initiatives (88%).

The SEC is not hearing profound seriousness to the cyber-security problem. It is time to move forward with professional CISO, CIO, and CRO positions reporting to the Board or CEO. We can do better, and the payoff is profound. Aon found that 30 organizations saw up to a 21% hit to financial performance following a cyber event – total value loss of $670 billion (9% drop in shareholder value). Seventeen organizations who responded proactively to an event saw an average increase of 18% over market norms – a combined increase of $445 billion. Integrated Risk Management produces cash to the bottom line.

Ramsomware and AI

Ransomware risk is now provided by 2 new actors with profound skill and creativity. The GoAnywhere and MOVEit organizations accounted for about 10% of the cyber and ransomware attacks in the first half of the year. These actors are talented in planting vulnerabilities in file-transfer tools which enable movement throughout an information system. The average cost of a ransom attack is now $2.51 million. Investment in cyber security resources and risk management governance is a wise choice.

Advanced Intelligence (AI) enables cyber-attack actors to more quickly and deeply design ransomware that skirts existing protection systems. Proactive deployment of end-point and systems security, remote work protections of VPN, application level security, access control, and data security produces a payoff. ZeroTrust protocol is worth exploring to minimize cross-system movement of threats and strengthen third-party and supply chain risk management.

Ultimately Business Interruption and Response Planning remains imperative to your business success. Risk Management governance is key, and we are here to help.

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

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 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!

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