Integrated Risk Management Solutions, LLC

James E. Blair, President

December 2015

Dear Colleague;

Our Clients ARE Working On Risk Priorities

A year ago we reported the top 5 Risk Management priorities defined by our clients. They were 1) Reputation, 2) Cyber Risk, 3) Behavior Risk (employees, suppliers and clients), 4) Business Disruption Risk and 5) Cash Flow Risk. Clients have deployed the Risk Management Executive Council governance process to prioritize material risks, initiate risk mitigation programs, align risk activities across organization silos, measure the performance of risk investments and anticipate evolving risks. This Advisory highlights the work of our clients to proactively manage the risks of their businesses.

Risk Management Executive Council (RMEC)

The RMEC governance process is being actively launched by clients. This Risk Governance team engages the top leaders of Operations, Finance, Sales, Legal and Human Resources (and IT where appropriate). The team prioritizes the organization's risk based upon the level of "materiality impact" and initiates risk mitigation programs championed by leaders that facilitate the organizational intelligence of cross-silo teams. Results of these programs are reported quarterly to the RMEC where progress is assessed, issues resolved, resources aligned, and emerging risks identified. Clients, both large and small, are establishing a rhythmic **90-90** theme which is a formal meeting of the RMEC every 90 days for 90 minutes. It is working!

Business Interruption Planning

The risks of business disruption impact several of the 5 client priorities. As an early initiative to mitigate risk, clients are developing Business Interruption Plans (BIP) that defines the organizational response to disruptions. Paramount are the **3 R's** of **R**ecognize, **R**espond and **R**ecover. Clients are working with suppliers/vendors and team members to emphasize the need for vigilant risk awareness that **R**ecognizes warning signs/disruptions and then urgently reports situations to an Emergency Response Team (ERT). Most clients have assigned the ERT operations to the RMEC.

Clients are devoting resources and training to more effectively **R**espond to disruptions. Table-top exercises present disruptive scenarios to the ERT in order to refine skills of quick decision making and engagement of team leaders and external vendor support for effective response. Communications plans are outlined that enable early reporting to executives, team members, clients, vendor/suppliers and the public (as appropriate). The processes of **R**ecognize and **R**espond lead to effective **R**ecovery.

Clients have prioritized the BIP and are making progress with oversight by the RMEC.

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

Cyber Risk

The FBI cites 2 kinds of companies: "those that have been hacked and know it" and "those that have been hacked and don't." This is a major risk fact! Malware swirls around the internet like dust in the wind and it lands where-ever an opening is found. Millions of personal information records have been pirated this year by global hackers, principally Health Care & Employee Benefits, Financial and Education sectors.

The breach of the U.S. Office of Personnel Management (OPM) exposed more than 24 million current and former employees' personal records to the Dark Web where the information will be resold for a lifetime. This breach is so massive that 6 months of work has been required to notify the affected parties of the breach and the systems available for ongoing protection. More than 100,000 tax payers were the subject of data breaches and hackers pirated $50 million in illegal refunds. Several clients were directly impacted by both the OPM and IRS hacks.

Regulators challenged Wyndham Hotels which was hacked 3 times during the 2008-2010, impacting more than 600,000 credit card users. The Federal Trade Commission (FTC) took regulatory action and the chain decided to litigate the Commission's enforcement authority. Wyndham lost and has entered into a 20 year compliance plan. Federal Government compliance plans are a tremendous expense and distraction!

Clients are recognizing the speed, depth and breadth of information breaches. Effective Risk Management requires early warning, sharp recognition and response. Leaders must know immediately about indications of a data breach (before anyone else), and then deploy BIP processes under the stewardship of the ERT. Clients are refining plans to **R**ecognize and **R**espond, communicate, deploy forensics talent to assess the damage, repair/recover, notify/report and prepare for elongated legal action. Some are deploying Cyber insurance to help cover costs (this is uncharted water, so please call us).

Emerging Risk - Physical Violence

The Paris, Planned Parenthood and San Bernardino shootings are another warning for your business. We will address this more in the 2016, but please review the Active Shooter Guide video https://www.youtube.com/watch?v=5VcSwejU2D0 and consider introduction of the Personal Preparedness Plan (PRP) found on our website at: www.integratedrisksolutions.com/uploads/Personal_Response_Plan_12.15.15.pdf

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