Integrated Risk Management Solutions, LLC

James E. Blair, President

Sept. 2017

Dear Colleague;

The Perpetual Risk - SILOS!

The year 2017 has presented just about as many risks as can be imagined. The US has now experienced the damage from hurricanes Harvey and Irma (we await the outcome of Jose and Katia), more than 1 million acres of wild fire damage, severe flooding, hail and crop damage from freezing weather. Millions of fellow citizens have been evacuated and a large percentage can no longer live in their homes. Businesses are disrupted from damage, unpredictable supply chains and the reality that employees may not be able to return to work while they attend to their families and property. Insurance and FEMA officials estimate total losses to date nearing $200 billion, and likely more.

If the physical damages aren't enough, prior to the Equifax announcement of last week, cyber breaches increased 24% over 2016, with a year-to-date total of about 17 million records stolen or compromised. Now, add the 143 million records breached from Equifax and the math is a 14X increase year-year. The magnitude is incomprehensible.

The lesson is that risk surrounds us. Its build into every business and personal decision we make. Remember "we take risk to generate cash – we spend cash when risk is not managed".

Risk = Cash!

Risks come in all forms, and our experience of 2017 is of extraordinary magnitude. The physical and business damages from unusually harsh weather are often unpredictable and mostly uncontrollable. The information damages from the cyber-breach attacks are becoming predictable and many are controllable. The test is how well we anticipate and prepare to holistically prevent intrusions, and then respond when bad stuff happens.

So why the emphasis on SILOS?

Organizational SILOS are the largest perpetual risk. When severe damage results from uncontrollable factors, the efficiency of Recognition and Response is sub-optimized, and often leaves a business in a confused and unresponsive state. The ultimate test of any organization is the speedy and coordinated Recovery from a severe disruption. Those that proactively prepare for and practice scenarios "Recognize, Respond and Recover" more efficiently than competitors. Silos tend to get in the way of prioritization, decision making, collaboration and action. Only a cross-SILO governance process can bring leadership and efficient resolution to the Response and Recovery efforts.

SILOS inhibit effective anticipation of emerging risks. Cyber-breach prevention, preparedness and response can only be accomplished by a cross-SILO governance process that engages all members of the organization in prioritizing the training, recognition and reporting of data-intrusions, phishing attempts and unexpected activity within the company information systems.

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

Industry has now discovered that technology alone cannot predict and prevent all cyber-breaches. Entrances into your information systems include employees, vendors, trusted partners, interconnections with peers, phishing by "bad guys" and websites. The Equifax breach appears to have been caused by a compromised website that then enabled hackers to enter the heart of the operating systems and sensitive data files.

Remember the bad guys are smart, and they understand the ineffectiveness of a SILO'd organization. Here are the top 5 reasons that cyber-security is ineffective:

1. Cyber-security is an IT problem! (not so - it's everyone's problem!),
2. Enterprise Risk Management does not exist or does not have visibility into SILOs,
3. Security procedures cause inconvenience,
4. Risk related data is not used for strategic decision-making,
5. Executives face "choice overload" – many vendors selling pieces of the solution.

The solution is a cross-SILO Risk Management governance process that brings leadership to the recognition of risks, prioritization of initiatives, performance oversight of risk functions, early Recognition of issues, Response and Recovery efforts. The benefits to the business from an Executive led Risk Management Governance process are improved client service, stabilized employee and vendor resources, timely recovery of operations, distinguished reputation and improved earnings. Attached please find the recommendations for Risk Based Cyber-Security Preparedness.

Beyond SILOs, one of the most pressing risks you face is a labor shortage. Following recovery from the last recession, job growth has steadily increased for 83 consecutive months (unemployment rate of 4.3%). Businesses are facing acute shortages of both labor and talent. CFOs suggest that business growth is being constrained by insufficient management time and talent. A Risk? You bet!

Risk based solutions might include – empowering your teams to be risk:

- aware
- creative (find solutions that minimize risk)
- trained
- responsive
- independent
- collaborative
- recruiters (find new talent)

Everyone is part of the risk-taking process, and can/should be part of the Risk Management team. The culture becomes one of risk awareness that strengthens the core of the organization to be more resilient in times of challenge.

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

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

Risk Based Cyber-Security Preparedness

Recommended Steps:

1. Diagram your information system network and architecture. A basic box and line diagram will do (use a cloud for "The Cloud"). Involve your team in identifying the components and leave no stone unturned, particularly connections with vendors and customers (including Cloud service providers).
2. Outline how transactions are processed and orders fulfilled using the components of your systems.
3. Identify all information/data owned and operated by your organization. This includes internal information (e.g. HR and Finance) and external information (e.g. customer locations, ordering and fulfillment processes, billing, procurement). Determine the "owner" of all information and evaluate the risks and value of the data (assign a risk materiality score to each segment of data based on likelihood of breach and financial impact).
4. Determine the current level of risk protection for the data and deploy mitigation strategies prioritized by materiality impact.
5. Establish unique security protocols for information segments according to the assessment (item 3). High risk information should be segregated and independently protected by internal firewalls and/or encryption.
6. Form a Cyber-Security Risk Governance process to oversee all matters related to information/data management in the enterprise. This process evaluates risk, prioritizes risk mitigation programs, measures performance and anticipates emerging risks.
7. Deploy cyber-operational monitoring that reports 7X24 performance of software and applications functions. Establish the concept of identifying anomalies which are the indicators of a potential breach.
8. The governance process formalizes an Emergency Response Plan to respond when indicators suggest the need for responsive action.
9. Monitor social media for external indicators of outsiders/insiders who might want to damage your business. Monitor tweets, social media criticisms, threatening Emojis, Google Alerts, Glass Door, etc. for unexpected statements that target the organization. Monitor security patching delays.
10. Train all employees to follow procedures and help monitor for anomalies.

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

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 incurred in multiple corporate silos hiding the "Total Cost of Risk."
- 75% of company information system risks come from employees and trusted vendors.
- FM Global, a world-wide property insurance and engineering firm, recently estimated that company earnings volatility can be reduced by 50% through effective Risk Management prevention and preparedness programs.
- In 2016, 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 well 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.

2017 Global Risks Defined by:

World Economic Forum

- Extreme weather events
- Water crisis
- Natural disasters
- Failure of climate-change mitigation & adaptation
- Large scale involuntary migration
- Terrorist attacks
- Interstate conflict
- Un/under employment
- Cyber attacks
- Man-made environment disasters

Executive Opinion Survey*

- Un/under employment
- Energy price shock
- Fiscal crisis
- Failure of national governance
- Profound social instability
- Failure of financial mechanisms
- Terrorist attacks
- Failure of critical infrastructures
- Asset bubble
- Cyber attacks

* WEO Survey 2017

Manage Your Risks Well!

P.O. Box 334
303-795-9754 (O)
Littleton, CO 80160-0034
303-734-1814 (F)
www.integratedrisksolutions.com
jeblair@integratedrisksolutions.com
303-886-8450 (C)