Integrated Risk Management Solutions, LLC

James E. Blair, President

June 2017

Dear Colleague;

Risk Based Cyber-Security!

Have you heard that Information and Data breaches (cyber-breaches) occur every minute? Daily news services report major (and minor) data thefts, manipulation, contamination and miss-use. The public has experienced miss-use of business and personal data at a rate that is growing 15-20% annually (small business up 40% over 2016). If you have not experienced a data hack of your company or personal information you are one in a million, or you don't know about it.

The magnitude of data breaches is so large that we may become numb to the daily throb of reports. Governments and Departments of Defense are as susceptible as the local 7-11 store. Small business/organizations are particularly vulnerable because they don't have IT staffs or substantial IT budgets for software, firmware and security systems. And, the primary culprits are employees and vendors who make mistakes or miss-use the company computer systems. Note: the shutdown of British Airways on Memorial Day weekend was a human error not a cyber-breach.

The bad guys continue to sophisticate their operations and refine approaches to pierce company/organization security architectures. The days of depending on the "old firewall" protection systems are over and organizations must now combine technology and software with policies, procedures, monitoring, analysis and governance to ward off attacks that arrive by the second (one client tallies multiple-millions of hacking attempts daily). Upon the very high probability that a hacking attempt will get into your information systems, the deployment of Response and Recovery operations is a new business imperative. Remember, the winners in the Risk Management race are those that Recognize and Respond faster than competitors. Combined with speedy Recovery, these organizations differentiate from the pack.

Risk Based Regulation

It's no surprise that global and local regulators are expanding consumer protections to guard against the damage of cyber-attacks. New requirements are being imposed on organizations of all sizes that require expanded operational and governance approaches to information security. The two new regulations are from the New York Department of Financial Services (NYDFS) requirements on financial institutions (effective 3/1/17) and the General Data Protection Regulations (GDPR) to be implemented in 2018 across the European Union (EU). The Colorado Division of Securities has proposed new rules on investment advisors and broker-dealers (April 2017).

These regulations align with the work of the National Institute of Standards and Technology (NIST) that developed a Critical Infrastructure Framework in 2014. These 3 sets of requirements/recommendations emphasize Risk Based principles.

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 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.

The wisdom of the RISK BASED regulations confirms the value of Integrated/Proactive Risk Management. The ROI is HUGE!

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

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