Integrated Risk Management Solutions, LLC

James E. Blair, President

December 2016

Dear Colleague;

The Cyber-Beat Goes On!

Our June 2016 Advisory outlined the 14 expensive steps required when a data breach occurs. http://www.integratedrisksolutions.com/uploads/Dear_Colleague_6.14.16.pdf

Since June innumerable data breaches have continued and at a pace that Kaspersky now estimates is one every 40 seconds. Your business is being attacked more often than once per minute. It's mind numbing; like swatting mosquitos. The new concept of "cyber-fatigue" is setting in. If it were simply a pest, we could all be happy, but these attacks are targeting the heart of your business including your bank accounts, customer lists, credit card accounts, employee health records, payroll records, business plans, Intellectual Property, tax returns, supply chain, AP/AR records and more. It costs the bad guys nothing to ruin your hard-earned business (their process is digital and runs 24X365 – non-stop!).

New victims have been breached since our last Advisory, including the BIG guys of Yahoo – 1 billion accounts; Google/Android -1 million accounts; LinkedIn, Dropbox, the USOC, US Dept. of Housing, Boeing Credit Union, Primerica, Chicago Public Schools, Michigan State University, State Street Bank and thousands of small to mid-sized businesses and institutions. Year-to-date, 900 formal reports of breaches have been made to the Identity Theft Resource Center (ITRC) involving more than 34 million records, excluding Yahoo. Ponemon estimates the cost of a breached record is now more than $200; so, 34 million X $200 = $6.8 billion, or so! At an average of $5.8 million per breach, cyber-security is worth prioritizing as one of your most important operating risks. Please consider - https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

The insurance industry is at a loss about how to help. Policies are written for coverage that is "unknown" since hackers operate at the speed of light and underwriters and policy designers operate at the speed of analysis. A positive is that larger insurers are partnering with IT security professionals from IBM, BAE Systems, Symantec and Accuvent/FishNet to consult and provide advisory services to larger clients – expensive! Most fundamental is that Technology **Will Not** Protect your business – People **Will** Protect your business!

Integrated Risk Management Solutions, LLC offers risk consulting and advisory services that engage your native "Organizational Intelligence" to develop and deploy holistic solutions to Cyber-Risk and all other operational risks. Since Cyber-Risk is one of the most rapidly developing risks to your business, and potentially one of the most damaging (National Institute of Standards and Technology "NIST" estimates that 60% of small businesses will fail within 6 months of a data breach), we offer you the following:

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

Steps to Prevent and Prepare for a Cyber - breach

1. Develop an Information Security Policy and Program that establishes procedures, training, follow-up and reporting for all employees and vendors.
2. Inventory your data and segment access to information to those with a need to know. Encrypt sensitive information (HR, IP, financial records, strategic plans).
3. Deploy Two-Step Authentication and complex passwords that are changed every 90-180 days.
4. Formulate a Risk Governance team that leads holistic approaches to Information Security, data breach response planning and other enterprise-wide risks. The team meets every 90 days for 90 minutes to address risk issues.
5. Consider the value of Cyber-insurance to cover the costs of a data breach that were outlined in our June 2016 Advisory.

As we look toward 2017, the following picture is emerging:

1. The Internet of Things ("IoT") is presenting cyber-risks at a rapid pace. Manufacturers are building micro-products with little security and hackers have simple access to these devices that are easily connected to the internet (20 billion IoT devices connected to the cloud). Ransomware will grow in sophistication.
2. Small businesses face increasing threats because a) they don't have security technology and b) may not have the IT talent in house to effectively protect the organization. They are targets if they have access to client's sensitive systems.
3. The evolution of Smart Cities deploying IoT devices that can control utilities, communications, traffic and emergency services will become increased targets.
4. Use of Artificial Intelligence (AI) to predict data breaches will emerge. Equally, use of AI by the bad guys presents an ever-increasing threat.
5. The education gap is increasing. We face a critical cyber skills shortage (estimated 10,000 in Colorado alone) and educational institutions must rapidly develop programs at the technical and university levels.

Small Business Guide is at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Cyber-Risk as an organizational risk can be effectively managed. The establishment of a Risk Governance process that identifies cash impacting risks to the business, prioritizes risk mitigation initiatives, measures results, and anticipates emerging risks is one of the most strategic improvements an organization can make. The native Organizational Intelligence of the business is amplified and results in a "Well Risk Managed Business". *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.

2016 Global Risks Defined by:

World Economic Forum

- Involuntary human migration
- Failure climate change mitigation
- Water crisis
- Profound social/political instability
- Cyber-attacks – Data theft
- Interstate conflicts
- Bio-diversity/eco-system collapse
- Energy price shock
- Extreme weather
- Major natural catastrophes

Executive Opinion Survey*

- Asset bubble, deflation
- Energy price shock
- Food/water crisis
- Involuntary human migration
- Social instability
- Natural catastrophe/weather
- Failure national governance
- Cyber-attacks
- Interstate conflicts
- Failure financial mechanics

**WEO Survey January 2016*

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