Integrated Risk Management Solutions, LLC

James E. Blair, President

September 2014

Dear Colleague;

So Your Business Has Been Hacked!

The probability that your business has suffered a data breach or service disruption is growing at an unbelievable rate. Data breaches are costing an average of $5.8M (up from $5.4M in 2013) and it's time to prepare for the time your business is attacked.

All the money that has been spent on prevention technology, outsourcing, firewalls and software cannot out-run the global hacking network. Every investment is being countered by equal and relentless sophistication by the "bad guys". *Well Risk Managed* organizations deploy a top-level governance process, written policies, employee training, intense system monitoring and engage an "All-Eyes-On-All-The-Time" culture with employees and service providers. These actions can slow the inevitable, but likely not prevent on a long term bases. This letter outlines the:

Five Steps to Manage a Data Breach

1. Monitoring – You must strive to know about the breach first (before anyone else)!
   a. The IT community is masterful as selling the newest technology and the hacking community is equally skillful and often works ahead of new software/hardware solutions. Your challenge is the utilization of the security monitoring tools available within your technology suite and the services provided by outsourcing providers. Interestingly, IT service providers do not emphasize Security Monitoring services – you need to pursue the services from them.
   b. Engagement of the "All-Eyes-On-All-The-Time" expectation of employees and suppliers. No-one is better equipped to identify unusual activity than operating teams. When something unusual is spotted a timely report to the IT Help Desk is a business imperative.
   c. Monitoring results should become a regular reporting item to senior management, and the Risk Management Executive Council (RMEC). This single action will cascade the awareness of security to the entire organization.
2. Engage Top Management
   a. When unusual activity is identified early deployment of the Crisis Management Team should become the norm. The senior team or RMEC should engage in immediate discussion to initiate next steps, including preparation for communications with employees, customers and suppliers.
   b. Effective communications internally will enable quick response by employees and suppliers while needed forensics and repairs are initiated. Equip your customer contact resources to message with customers in order to protect long term relationships.

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

3. Forensic analysis and repair of the compromised systems must:
   a. Be conducted by appropriate Subject Matter Experts. The organization should maintain immediate access to these resources to assure early deployment.
   b. Determine the facts and extent of the situation and implement repairs.
   c. Provide regular updates to the RMEC.
   d. A plan for Disruption of Service to protect others may be appropriate. As uncomfortable as "unplugging" the system may seem customers will appreciate the interruption more than the long-term effects of the data breach.
4. Report the breach externally as required by your regulators, and as appropriate to garner support from law enforcement. The FBI for example can provide significant forensic support to help identify the origin of the hackers. In addition:
   a. Be aware that 46 States have specific reporting requirements.
   b. Significant value comes from a predetermined plan. Legal counsel can help determine what and who needs to be alerted to a breach.
   c. Pre-determine the priority and list of communications stakeholders, including Suppliers, Service providers, financial institutions and others affected.
   d. Notify your Cyber-Insurance carrier, if appropriate.
5. Customer Care is imperative to managing the reputation damage from the breach.
   a. A pre-planned communications initiative for your customers is a major asset.
   b. Help customers manage their fears and bolster confidence in your ability to repair the breach and protect their financial well-being.
   c. Communicate with increasing regularity, with time schedules to report progress.
   d. Consider refunds/credits for services that were compromised (and not delivered).
   e. Offer Credit Protection services for up to 24 months.
   f. Communicate – Communicate – Communicate

The lesson from Target and E-Bay, and now Home Depot, is the need for an effective Risk Governance structure that identifies and prioritizes organizational risks, aligns mitigation programs, measures results and proactively discovers emerging risks. When the unexpected occurs, the governance process deploys the **3 R's** of Information Breach management – early Recognition, Response and Recovery.

Integrated Risk Management Solutions provides the Risk Management Advisory services to help you 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 2014, 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.
- 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.

2014 Global Risks Defined by:

World Economic Forum

- Fiscal Crisis in Key Economies
- High (un/under) employment
- Water crisis
- Severe income disparity
- Climate change
- Extreme weather events
- Global governance failure
- Food crisis
- Failure major finance institution
- Profound political/social instability

U.S. Business Leaders*

- Business disruption
- Supply Chain
- Natural catastrophes
- Cyber incidents
- Reputation damage
- Environmental issues
- Talent shortages
- Global pandemic
- Food/water/Energy shortages
- Regulation

**Allianz Risk Barometer January 14, 2014*

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