Integrated Risk Management Solutions, LLC

James E. Blair, President

June 2016

Dear Colleague;

Responding to an Information Breach
14 Expensive Steps!

Clients are increasingly bewildered about actions required upon the discovery that their information systems have been breach. No longer can we plan on networks and data being protected – attention must turn to the day a breach occurs and actions that leaders must take to meet customer expectations and regulatory requirements.

Your information resides everywhere and technology has made it overly easy to save and store anything anywhere. Most clients don't know what information they have or where it is stored. A comprehensive inventory of corporate information and the systems utilized for storage and processing is becoming a "must have!"

Examples of critical information include:

- Intellectual Property	- Patents, Trade Secrets, Copyrights	- M&A Plans
- Financial Plans	- Strategic Plans	- Board Records
- Corporate Records	- Banking & Financial Records	- Employment Data
- HIPPA/HITECH	- Personally Identifiable Info. (PII)	- PCI/Credit Cards
- FERPA Student Info.	- Vendor-Customer Info.	- System Records

Hackers and nation-state operators are scanning the global networks 7X24 to find openings in your network to hide a malware bot that will erupt at any time and leak your information into their hands, or perhaps corrupt your information making it useless and/or dangerous to human or corporate health. Growth in this industry is an alarming 150-300% annually and costing the global economy more than $445 billion in 2016.

I am finding that clients have invested heavily in their information systems over the past 10 – 15 years. The investments have been incremental with new additions annually. Often these accumulate into a network of disparate systems that don't lend easily to coordinated control, management or maintenance. Consider the Manufacturing Digital Controls (SCADA) systems that wind throughout manufacturing and service organizations. They have been placed in operations for years and few remember how and who made the installations, limiting effective maintenance, updates and patches.

Steps Required to Respond to a Breach

With everything you have put into the health and resiliency of your information systems and with the conditions just outlined, preparations should be made for the day you must respond to an information breach. These preparations and plans should be under the stewardship of a Risk Management Governance Council which we have presented in most Client Advisories from *Integrated Risk Management Solutions, LLC*.

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

Here we go – please consider all 14:

1. Breach Detection – Application level detection is critical to detect within hours.
2. Forensic Analysis – What, where, by whom, and who is impacted - 1-3 days.
3. Repair – The level of damage and the fixes needed to get back online within your Business Interruption Plan – 2-4 days.
4. Identification of Parties affected – Customers, vendors, employees, shareholders – 5-10 days.
5. Legal Protection – Establish an Attorney-Client Privilege protocol to protect the details of your investigation and action steps (anticipates longer-term litigation).
6. Communications Plan – Pre-prepared communications for internal and external stakeholders – 1-3 days.
7. Notify Regulators – 48 States require notification of the Attorney General and the affected parties within a "reasonable" period – 30-45 days.
8. Notify Parties – Initiate a paper mailing notification of affected parties. Establish an 800# call center to respond to inquiries. This process took 12 months for the U.S. Office of Personnel Management breach (24 million individuals).
9. Credit Monitoring – Offer services to affected parties as a matter of client relations.
10. Identity Repair – Offer services to affected parties as a matter of client relations.
11. PCI Analysis and Repair of Systems – The Credit Card providers oversee your credit card processing and will expect thorough reports of the findings in item 2 and 3. Expect heavy fines and penalties.
12. Regulatory Examination and Fines – Prepare with legal counsel for fairly heavy handed regulatory penalties.
13. Litigation – Insurers are hesitant to write many cyber-policies because of the unknown and lengthy "tail" liabilities that will accrue over 5-10 years.
14. Reputation Recovery – Your organization's name will be on the news and internet. You can't hide from an information breach. Reputation Recovery starts with the Communications Plan listed in item 6. Chipotle is spending $100 million or more to recover their brand reputation following the health scare from E. Coli.

The damage from information breaches is serious. Ponemon estimates the cost per record breached (to pay for the 14 steps) is now $201, and average total cost per incident at $5.85 million. On the other hand, Risk Management is not expensive! The Governance process amplifies "Native Organizational Intelligence" in a manner that strengthens the business and its constituents.

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