CloudCover™

2999 County Road 42W - #200
Burnsville, MN 55306-6995
Fax 877-532-0390

December 15, 2013

To: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

From: Stephen Cardot
Chief Executive Officer
CloudCover®
2999 County Road 42 West, Ste 200
Burnsville, MN 55306

Re: Data Governance, Compliance Automation, and Risk Transfer. Where are these terms?

Dear Mr. Sedgewick,

Today's corporate leaders face multiple challenges, including the need to innovate in extremely competitive business climates, address highly dynamic regulatory and compliance challenges, and secure the enterprise against a wide barrage of new and evolving sophisticated cyber threats.

Even though responsibility for risk management guidance is entitled upon the Cybersecurity Framework, we should remind ourselves that cyber security practices today are already influenced by data governance, risk transfer and compliance automation initiatives. Yet this specific language is missing from the Framework.

Take for example the data governance practice. Data governance is a fairly new risk practice that specifically activates data security. It can address data ownership and feasibility and can further support the basic tenets of the Framework — Identify, Protect, Detect, Respond, and Recover. Data governance, in terms of cyber security encompasses people, processes, and information technology required to create a consistent and proper handling of an organization's data security posture and the risk handling of data across the business enterprise. Data governance initiatives improve data security and quality of cyber security adoption by assigning a team responsible for data's security, accuracy, accessibility, consistency, and completeness, among other outcome-focus performance metrics.

Data governance today is currently becoming the most discussed effective risk managed practice within Fortune 100 financial companies in the U.S. and EU. So, why are major businesses practicing a new risk management model, not mentioned without any representation, within the Preliminary Cybersecurity Framework?

Data governance is more than the oversight role or the process by which organizations manage and mitigate data risk. It has become the risk management role, which allows an organization to evaluate all relevant business and regulatory risk controls and monitors mitigating actions in cyber securable ‘data centric’ industries such as banking or health care. There is only reference to governance, and yet “data governance” is missing in language or clarity.

Successful organizations are beginning to understand a greater percentage of their cyber risks at a deeper, more data risk centric level, which require better risk measurable tools. That understanding is also beginning to lead to having a more proper data governance practice in place — such as continuous monitoring, or decision-making execution strategies that are more automatic and ready to meet compliance, forensics, restoration and tailored incident response events for real time action. This now brings us to compliance automation.

Compliance Automation is about how, what, where and when to automate the control verification and streamline internal and external audit challenges near real-time response processes. The compliance automation list is inline with cyber management initiatives and should include the means to:

- Adapt to existing cyber security, governance and auditing processes — real time
- Respond to complex and rapidly changing cyber risk environments in real time
- Meet auditing and data management standards near real time
- Identify control gaps and prioritize incident response

Security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed around risk challenges today. Compliance is also an obstacle to efficient data security, cyber risk visibility and mitigation, as well as real-time Netflows. Real-time compliance becomes the sought after grail — the real answer. Compliance automation delivers best practice compliance observance in real-time result.

Data risk compliance for the sake of privacy, therefore, has become the higher common “denominator”, with the most aggressive data privacy mandates driving corporate risk management strategies toward a more robust continuous risk mitigating automation model. In order for an organization to adhere to new data privacy demands, United States companies requires a robust information security framework that delivers comprehensive protection across all security domains within their purview. Active compliance to regulatory standards across jurisdictional domains in the United States and also recognition of the newer data policy protections in the EU, demand a more flexible identification and functional framework.

Therefore, the best cyber security approach is to adopt a risk-reduction strategy through the implementation of an active “real time” functioning solution that allows an organization to prioritize security and compliance efforts based on data-centric risks. As a result, through a real time data governance and compliance automation initiative the risk management process provides a strategic orientation for companies of all sizes, in all geographies with a formal process to identify, measure and manage risk.

With that said, we now come to risk transfer. Risk management principles should address risk mitigation that begets loss control that begets risk transfer. Risk transfer comes in behind loss control as a gap satisfier, not just a recovery funding mechanism. Risk transfer is a qualifier and a metric for risk quantification. Again, risk transfer should not be considered a risk recovery protocol. But, as a risk transfer agent inventively pushing more effective loss control. However, when everything has gone “data breach” then risk transfer’s adjudication ability is the appropriate financial funding mechanism to address “data loss” recovers or make whole. Therefore, recover is a practical function in security. But, it does not complete the circle of cyber risk logic. There is something missing.

Where is the Sustenance Tenet?

Sustainability is not yet an autonomous field or discipline of its own, and has tended to be problem-driven and oriented towards guiding decision-making and measurement. Cyber Sustainable Security is a term that denotes cyber security as on-going requirement for sustainable operations and is measured on the quantitative basis for the informed real time management of sustaining cyber security parlance.

The metrics used for the measurement of cyber sustainability (involving the sustainability of information technology systems, real time business and compliance domains, both individually and in various combinations) are evolving: they include indicators, benchmarks, audits, sustained standards and certification systems like indexes and accounting, as well as cyber risk assessment, appraisal and other reporting systems. Sustainable cyber business practices, on the other hand, integrate cyber security concerns with people, economic metrics and data governance.

Thus, sustenance —Identify, Protect, Detect, Respond, Recover, and Sustain — is the comprehensive frame-up that needs to be further developed.

Cybersecurity Framework should also offer insight to address some of the following questions that actually effect data security. Such as “Who owns the data?” “When is someone responsible or not responsible for the data that they handle?” “How and where should data be classified by cloud jurisdiction?” “What cyber security safeguards should be required by industry when handling personal identifiable information?” “What is defined as a catastrophic data breach?” “Why not define cloud computing as a cyber risk centric category?” “Why are there not risk transfer references within Recover?”

Simply put, governments, regulatory bodies, and consumers are concerned about data privacy and what steps organizations should take to proactively protect the security of their real time data, not learn far after a data breach that their data was a victim to loss or theft — due to an inadequate cyber security framework.

Thank you for your consideration and review.

Respectfully,

Stephen C. Cardot
Chief Executive Officer
CloudCover®