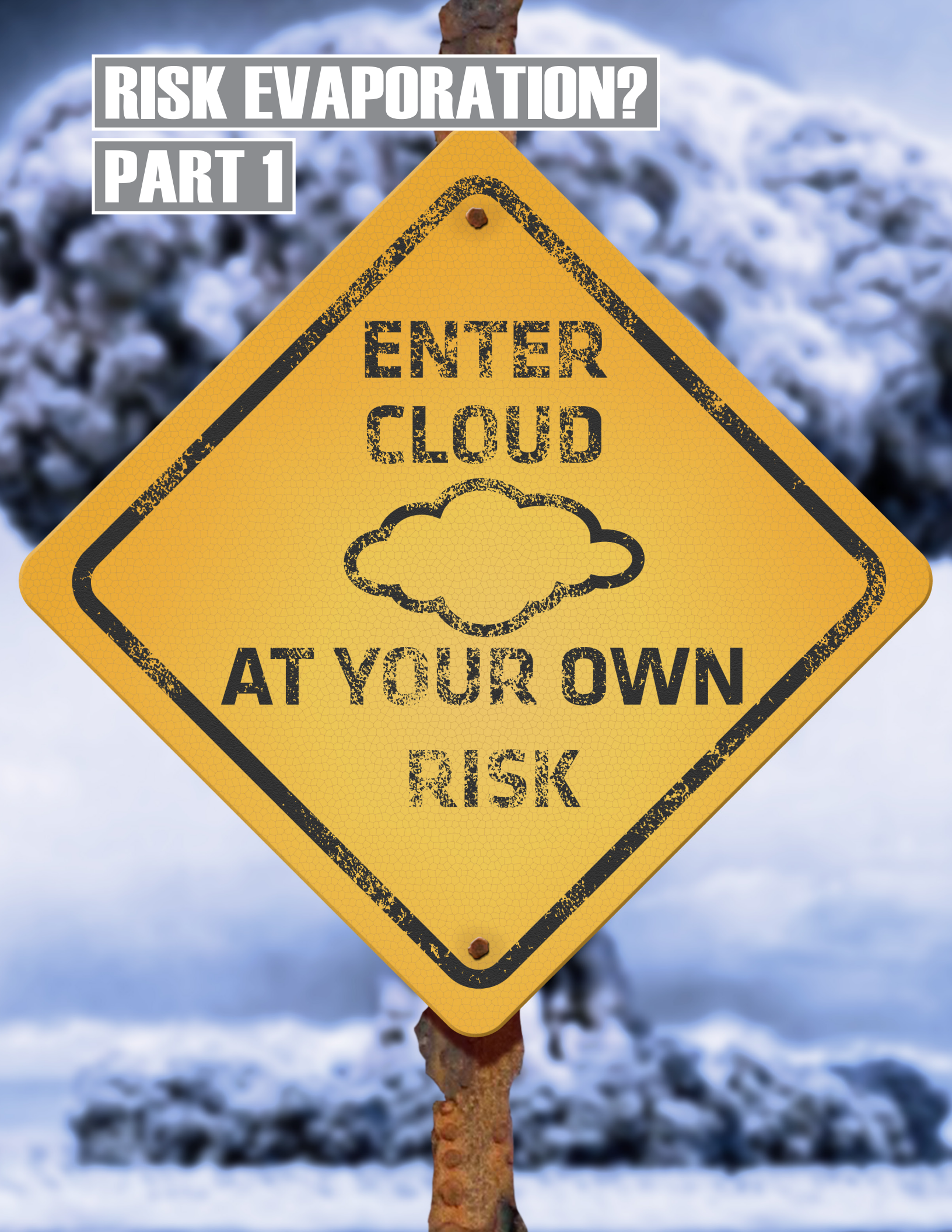
# RISK EVAPORATION?
# PART 1



# EMERGING CYBER RISKS: BETTER VISIBILITY FOR THE CLOUD FORECAST

By Drew Bartkiewicz and
Meghan McAuley Hannes

## FINANCIAL RISK PATTERNS IN CYBER SPACE

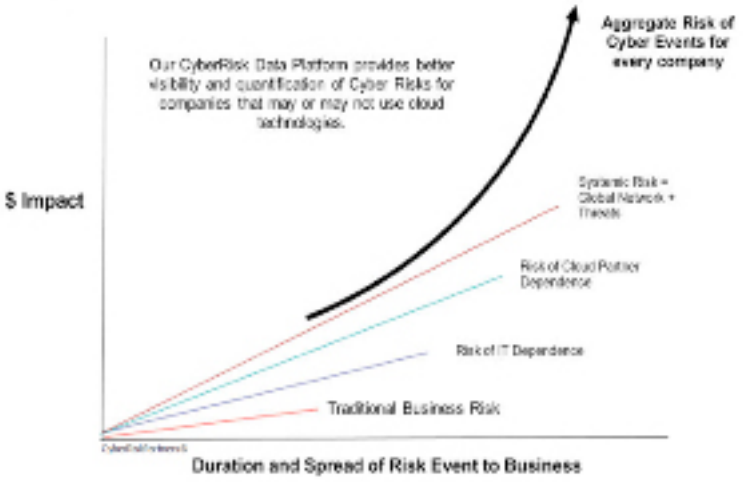
Virtually every established industry in the world presently involves risk transfer and massive insurance markets to absorb unexpected catastrophic financial or legal impacts, except for the cloud computing industry. Industries that rely on the insurance marketplace range from banking to property, energy to transportation; even the rental car industry relies on insurance for business-sustaining risk mitigation purposes. The cloud computing sector is an emerging industry with enormous promise with equally great unseen, aggregated financial liabilities. Prediction: The risk transfer marketplace for cloud computing will soon take hold through the powerful force of sheer, simple economics.

All industries in the world have risk, some are operational and others are more systemic. From time to time and within high-growth emerging industries like cloud computing, some market-leading companies can temporarily delay the financial risks to themselves (and to their clients) until the inevitable economics of risk exposure slow their own business growth. Risk denial is now running its course for the major cloud leaders, even though the business world is beginning to rely on the longer-term efficiencies of cloud computing now more than ever. This confluence of events – increasing risk against limited acknowledgment of its presence – creates both a problematic situation and an opportunistic area of growth for the cloud computing industry.

Free-trade economic supply and demand conditions implicitly rely on financial sustainability against risk uncertainty for continued success against the backdrop of regulatory intervention from unaffiliated entities. Undervalued and unacknowledged risk creates uncertainty in any marketplace. The uncertainties facing the current cloud computing marketplace are the questions surrounding key operational metrics such as data privacy, security and business interruption. The cloud marketplace as a whole faces challenges addressing and affirmatively answering for these uncertainties as cloud clients weigh the deeper cost-benefit advantage of cloud adoption.

## CLOUD COMPANIES ARE NOT IN THE BUSINESS OF RISK

Long-term successful performance by cloud companies and continued adoption of their services by cloud clients necessitates an affirmative answer to the following question: Who is financially liable when something unexpected occurs within cloud infrastructure? Both cloud companies and cloud users are spending valuable time and resources assessing what the insurance industry should have the capacity to answer. In fact, two parties are trying to solve what a third industry has previously mastered: risk valuation, risk hedging, and risk transfer.




## RISK VISIBILITY

Fundamentally, cloud service adoption means many organizations no longer need to invest in internal IT infrastructure to utilize various software packages, platform services, and data utilities. Because of the compelling economics of cloud technologies, companies are dispersing these business-critical functions to cloud companies – and they are handing over these responsibilities at a very rapid pace.

The current enigma here is that most cloud clients believe that the shift of computing resources and responsibilities to a cloud company includes the transference of the implied and inherent financial liabilities for data loss, data corruption and/or system interruption. This presumption is emphatically not true, and this presumption is especially concerning for cloud customers who are left little recourse for financial recovery in the event of cloud malpractice resulting in business-impacting liability.

When a cloud company becomes an outsourced provider, whether via a private, hybrid, or public cloud model, a fundamental shift in financial liability has not occurred even though data governance and infrastructure responsibilities have been transferred. Rather, cloud clients at present are positioned to financially absorb the failure, breach, or interruption of cloud companies. Clients have to underwrite each cloud they enter into an agreement with, because the operational business risk associated with choosing any number of various cloud companies now resides squarely on client balance sheets. The problem is that few cloud customers realize that the cost to use technology is rapidly being replaced by the growing cost to fail with technology. Whether the financial risks of data liabilities are accounted for or not, cloud customers are on the hook for cloud company

liabilities. This creates a problem for the cloud computing industry seeking more predictable outcomes.

## RELIANCE ON DATA ASSETS = ACCOUNTING FOR DATA LIABILITIES

The moment a cloud becomes a custodian of data (through an SLA, MSA or other actual or implied contract), the client has a burden resulting solely from the potential that the cloud company might "lose" that data. The exposure of data liability, however, remains the same just as if it were stored on the client's own internal IT systems. Except now, the data also resides in the cloud, creating a significant change in the risk mitigation options available to cloud clients. Total "data control" moves largely out of the reach of cloud clients, while leaving the data's financial liabilities squarely intact.

Clouds accept hardware, software and technology-scaling complexities to make money. Cloud customers clearly gain business efficiencies through scalable and largely consumable models for managing their data assets. As long as there are ongoing business risks and data liabilities associated with reliance on data assets, there is a need to value, allocate and account for the risk complexities the cloud market presents.

An obvious assumption is that the optimal financial outcome of any company is to completely avoid a cyber-event that creates financial loss, liability, or interruption. But in a world where even oil rigs can illustrate catastrophic impacts of operational hazards, risk-aggregating industries (like the cloud industry) need to acknowledge the inherent systemic risks within their business models. As the last decade has taught us, technology certainty cannot be guaranteed by technology alone. The times for IT risk, they are a changing. In the client-server world, technology errors and omissions had a built-in containment model that limited the event spread and impact. These were single-tenant architectures with a degree of isolation about them. The financial business risk was more operational than network-based or systemic. Catastrophic technology scenarios were even hard to contemplate. However, data patterns over the last few years have shown a noticeable uptick in financial consequences of our increasing technology dependence. Shared networks now mean shared risks. The cloud is clearly a "shared risk model" with the potential for cascading impacts. So, who is financially and legally responsible when cloud services result in a data leak, breach or outage: the tenants or the multi-tenant landlord?

## MEASURING RISK CURVES THROUGH ANALYTICS

CyberFactors™ is a predictive modeling and cyber risk intelligence platform to help businesses monitor emerging business risks of information technology and the world's largest cloud computing models. Highlighting the last few years in particular, CyberFactors™ data reveals cyber risk patterns that not only differ by industry (like healthcare and financial services) but also illustrate risk patterns that indicate an increase of cyber severity for virtually every industry...including and especially the clouds. With global cyber threats on the rise and the "cost to fail" with technology going up, this potential for cyber severity risk becomes not just a security challenge for cloud models but a financial challenge as well.

As cloud clients consider a major move to online applications and other cloud services, additional factors must be considered: the realities of multi-tenancy (or any shared infrastructure) and business-critical dependence on that infrastructure. DOS and DDOS attacks traditionally aimed at one company could now drastically impact the services of an unrelated, but co-located, firm within the cloud or a business partner of that victim organization (a la Wikileaks). Furthermore, international hackers have successfully penetrated the largest search engine in the world, gaining unauthorized access to highly sensitive, corporate confidential information by circumventing the very world-class security controls that were in place at the time of the attack to defend against such a situation. The case that a data breach or malicious attack can affect a cloud company and the greater cloud industry has been, and continues to be, made. Fortunately a market-shifting event in cloud confidence has not occurred. But why should cloud clients deny that their data assets and liabilities carry residual risk in the cloud? Developing effective financial protection to mitigate technology and data liabilities becomes difficult if no cloud-specific, risk transfer market currently exists…yet.

# STUCK IN THE RAIN

Regulatory requirements have been enacted recently to form a common code by which different industries must control the data they store, process and protect as a data custodian. These codes are commonly referred to as HIPAA, HiTech, SOX, State Notification Laws and Red-Flag Rules, to name just a few. When cloud clients collect any data from their clients that contain any variant of Nonpublic Personal Information, they are responsible for abiding by these codes. When cloud clients enter into a service agreement with any cloud company, they are entrusting and implicitly relying on that cloud with their data and infrastructure, their business livelihood, in some financially meaningful way.

Furthermore, cloud clients also face business-interruption and related liability costs that are associated with any inability to gain access to their data or infrastructure within the cloud. It is the cloud client "without the chair when the music stops" per se. Whether it's an idle workforce or transaction platform, a halted manufacturing process or the inability to conduct accounting or payment activities due to a cloud outage, clients are assuming the financial repercussions, relying on the 99.9 percent uptime "guarantees" embedded within SLA/MSA service agreements. However, what happens when their e-commerce website goes dark, for eight hours, seven days before Christmas? Where is the true financial recourse for lost income, lost productivity, lost customers and damaged reputation? Costs that far exceed the worth of any service obligation? The cost to fail with cloud technology in this instance has far exceeded the cost to utilize cloud technology. Getting a "service credit" for $1,000 is little comfort when a data breach could cost a cloud customer a $5 million liability.

So here is where things are heading in the world of cyber risk: shared risk and more innovative risk transfer mechanisms. The cloud clients now share the risk profile of their cloud service providers; the service providers now share a risk profile with their clients. But with the cost to fail going up rapidly, the business risk of data liability is not evaporating, it is merely being ignored.

Whether a customer risk profile is heightened or lowered with a client's entrance to the cloud is a moot point; the fact is that the potential for financial liability in the cloud will remain for as long as businesses (and consumers) value their own information assets. And if the financial liability of data still exists, a mitigation or transfer process for data risks must follow, as it does for every other industry, everyday around the globe. Reliance on the premise that clouds are better at security than their customers does not equate to evaporated financial risk. "Better" is not a guarantee to shareholders and customers alike, especially when the rising financial costs of data malpractice and system outages have no end in sight.

Traditional business risk models were perhaps created for a world that no longer exists. It is time to innovate. Into the clouds we all go. ■

# ADDITIONAL RESOURCES

1. Robert Lemos "Denial-of-Service Attacks Meet the Cloud: 4 Lessons" www.CIO.com November 2010

Part II of this article will be published in Cloudbook Journal Volume 2 Issue 2.