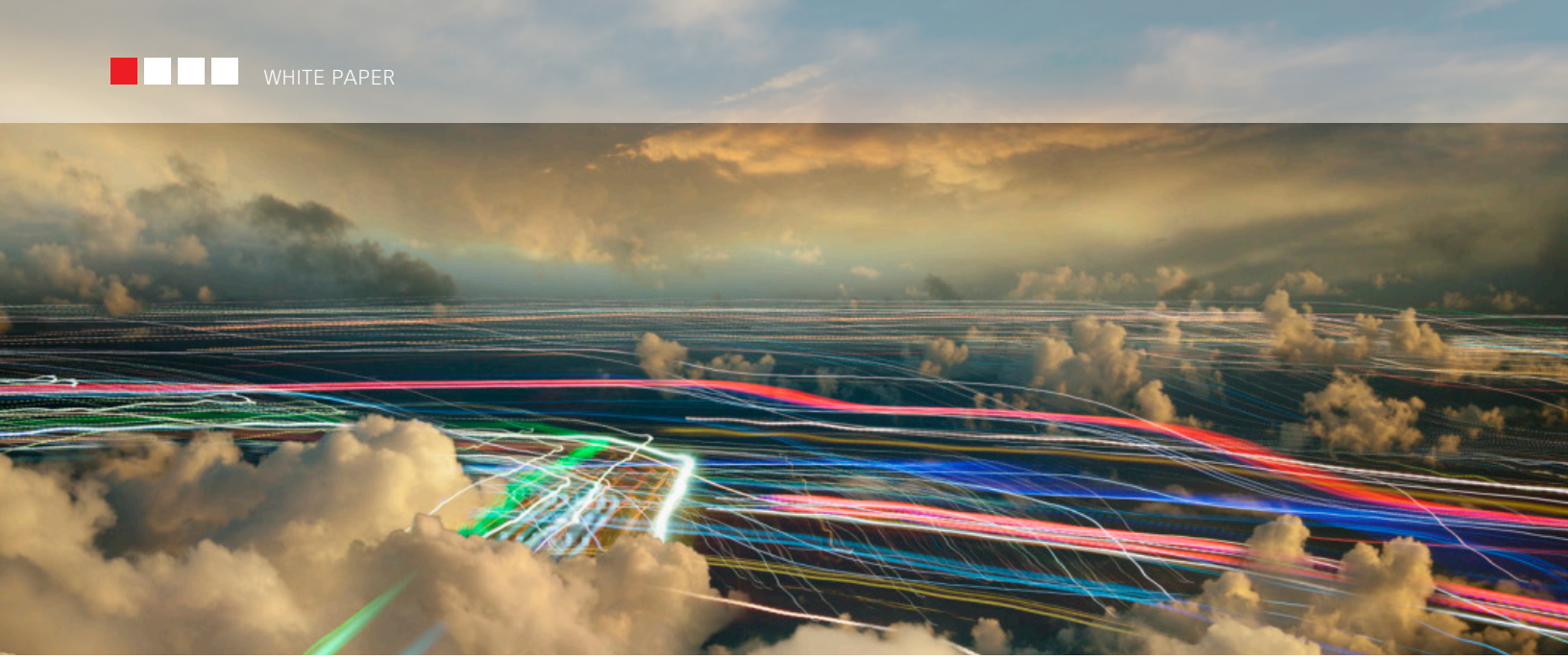

Perfect Storm Brewing

How insurance can help organizations protect their reputation and bottom line as the perfect storm of big data, cloud and mobility bears down.

TECHNOLOGY—LIKE FIREWALLS, FILTERS, PASSWORDS AND ENCRYPTION—cannot by itself help organizations understand exposures, identify vulnerabilities, hazards and triggers, and predict the severity and likelihood of a data loss. Indeed, after all the technology has been implemented, organizations are still left with the question: "How do we manage risk after we've done the basics?"

However, when combined with growing compliance issues, the potential for system failures as well as various security and privacy concerns, these often-interrelated trends are on a collision course. It's a collision that could result in the perfect storm, and ultimately irreparably damage the company's reputation, not to mention its bottom line.

So what steps can CIOs take to shield their organizations from potential damage? While instinctively seeking out additional tech solutions is part of the equation, having a robust risk management program and proper insurance coverage in place can provide safe harbor.

DIVING INTO DATA

To be nimble—with people at all levels making timely, sound decisions—organizations must provide better access to business data. As such, the statistics around big data are mind-boggling. For instance, IDC expects the big data market to grow from $3.2 billion in 2010 to $16.9 billion in 2015. In addition, the volume of business data worldwide, across all companies, should continue to double every 1.2 years.

All of this data opens up an array of exciting opportunities, including new revenue streams—perhaps none more exciting than developing new models to help others figure out how to best leverage their data.

However, there are also a number of questions businesses need to address. For instance, who owns the data? Was it gathered legally? With more businesses going global, data ownership and collection definitions can differ significantly, which compounds complexity. And as a result, the misuse, inappropriate storage or improper management of this information—or lack of awareness of laws that govern that data—can translate into regulatory actions from governing bodies.

CIO
Custom Solutions Group

ZURICH®

"Whether it is customer data, intellectual property or personally identifiable information, IT is responsible for considerably higher volumes of constantly moving data that's accessible from a growing number of points," says Gregg Fergot, vice president and head of technology with Zurich in North America, a global insurance provider of market-leading insurance solutions for technology companies ("Zurich"). "And at the end of the day, the key concern around big data is that when this information is mishandled or gets into the wrong hands, the company's reputation is at stake."

At the same time, while tracking customer activity from numerous access points creates a significant portion of today's information opportunity, businesses also can buy targeted data, including customer profiles and market analytics, explains Jim Charron, technology practice leader with Zurich. "In these instances, there could be questions of who really owns the data or whether or not compliant methods were used in its collection, which can differ significantly by country."

"Businesses are becoming increasingly mobile and the information residing on these devices all too often includes personally identifiable information, confidential data or even intellectual property."

— Jim Charron, technology practice leader, Zurich

Fortunately, there are insurance products available to provide protection. For instance, while Security and Privacy coverage was once reserved for firms within hospitality, medical and other environments conducive to collecting personally identifiable information, it can prove instrumental as organizations grapple with big data.

"First-party Security and Privacy coverage can provide for a breach coach, crisis management [including legal, public relations, advertising, forensics investigation, notification printing, credit monitoring, postage, etc.] as well as protection for business interruption and data destruction," says Fergot. "The third-party coverage also helps with the expense of being sued on top of dealing with the breach."

Furthermore, as groups like the Commerce Committee, chaired by U.S. Senator John Rockefeller (D-W.V.), continue to strengthen the legislation around big data and consumer protection, there is a growing need for strong risk management practices, explains Charron. "Categorizing this data by type, such as mission critical, corporate confidential, personally identifiable, etc., enables a company to make informed decisions about the legal, regulatory and business income risks they face with each data set."

IDENTIFYING STORM CLOUDS

While organizations are finding new ways to deal with and leverage the data explosion, cloud growth is taking data outsourcing into new realms, often with global implications.

For example, businesses may initially know where information resides, but providers move data regularly, explains Charron. "This becomes an issue if a hacker gains access, and security measures do not comply with local laws. It may require you to provide certain measures, including credit monitoring. This is something covered under Security and Privacy—whether data is in the U.S. or abroad."

However, with the cloud, the concern is not just around outsourcing data. As organizations move toward the cloud—whether it's a SaaS (software as a service), PaaS (platform as a service) or IaaS (infrastructure as a service) environment—security against hacks is a primary and valid concern. So much so that in the recent "(ISC)² Global Information Security Workforce Study," more than 80 percent of respondents cite confidential or sensitive data loss or leakage and exposure of confidential or sensitive information to unauthorized personnel as top cloud computing concerns.

"Because there is so much data in the cloud—especially the public cloud—hackers see these avenues as very attractive," says Charron. "And, eventually these [cloud] facilities will suffer an attack that will corrupt or destroy the data and shut down service."

First-party Security and Privacy coverage could apply whenever there is denial of service or inability to access a compromised cloud facility. "This is true whether denial of service means the organization is unable to provide services to its customer, or unable to continue accessing data needed for research and development activities," says Charron.

Third-party Security and Privacy coverage comes into play when a company is sued for its failure to provide contracted services to others as a result of cloud failure, explains Charron. For example, assume a software firm relies entirely on a public cloud provider to deliver an application to its customers. Should a hacker shut down the cloud facility, the software company is unable to fulfill its contractual obligations. In addition to the concerns around potential privacy exposure, this represents a breach of contract, opening the organization up to a lawsuit.

For many, cloud computing exposure also includes disruption in access (system failure) to subscribed software applications hosted in the cloud (SaaS) as a result of an act of God or another traditional property peril such as lightning, fire, wind, rain, floods and earthquakes. Hurricane Sandy serves as a prime example of late. "This loss of access can result in increased expenses and lost profits to the software company that contracted with the cloud service provider to host their applications," says Charron.

The big concern here is that most people do not necessarily know where their exposure lies because data often moves. "You may be a New York firm contracted with a large cloud service provider and assume your data will be in Virginia," he says. "However, it's possible your data will move to another location in Southern California. Unfortunately, you may not realize this until after an earthquake either damages data or prevents access."

According to Charron, understanding how much the data is worth is the most complex part of the equation when insuring cloud activities. "If the company purchased the data, it may not have tremendous value," he says. "However, there can be newly created data or intellectual property from designing code or insight derived from big data. When this data is corrupted or lost, the cost to research and recreate it can be substantial."

Whether a loss is due to traditional peril or cyber attack, cloud vendor contracts are quite clear in outlining their responsibility—and it's the actual data owner who is responsible for consequential expenses (i.e., notification, credit monitoring, breach coaching, etc.) in the event of a breach, explains Fergot. "Just because you are contracting with someone does not mean you relinquished your responsibility and can go without coverage," he says. "These companies have a lot of leverage and protect themselves against such expenses."

BATTEN DOWN THE MOBILE HATCHES

Mobility is also growing in leaps and bounds, contributing to the big data challenge. In fact, Gartner recently predicted a dramatic increase in IT spend for 2013 and beyond with device spending (laptops, tablets and smartphones, etc.) up 4.2 percent. In addition, the Bring Your Own Device (BYOD) trend shows 53 percent of organizations globally currently have employee- or partner-owned devices accessing business networks and data, according to the (ISC)² study.

As such, mobility leads to an increased number of access points, empowering more people with seamless access to data. While the benefits are quite attractive, the associated risks are equally substantial. Within a mobile culture, IT needs to provide security beyond its four walls—not an easy task considering that today's tablets and smartphones represent attractive access points for hacks and breaches.

"Businesses are becoming increasingly mobile and the information residing on these devices all too often includes personally identifiable information, confidential data or even intellectual property. The challenge is that this data is subject to certain laws and when you move it around it's hard to keep track of the differences in jurisdictional requirements," says Charron. "Risk management engineering can play a pivotal role by helping you determine what information to make portable and who to allow access."

According to Charron, as BYOD adds to the number of devices accessing business data, IT leaders need to focus on creating a safety culture around managing information. "Technology firms have a tendency to be overly confident, in part because they create the hardware and software," he says. "Every employee needs to recognize the vulnerabilities associated with having mobile access, how a data breach could impact the organization's reputation, and what steps they need to take to protect access. If not properly managed, these portable devices are attractive entry points for hackers, and could result in irreparable harm."

What's worse, this is an area where outdated insurance policies haven't kept up, says Charron. "While traditional policies provide cover for claims resulting from an insured's owned computer networks, coverage may not apply to the use of other networks, employee's smartphones or tablets," he says. "However, with specialized coverage, it's possible for businesses to be protected for all of their computing activities."

ALIGN WITH ZURICH

Managing reputational risk is about identifying vulnerabilities, applying controls and buying insurance where needed. That added coverage can pay out against direct damages, reimburse for remedies and help minimize the impact of exposure. And when you align with a company like Zurich for insurance coverage, your organization can focus on pursuing business opportunities—whether that's moving into new geographies or expanding the supply chain—with confidence.

THE RESULT: A PERFECT STORM

The potential for havoc heightens, particularly in the area of security and privacy, as an increasing number of employees use mobile devices to access and manipulate data through the cloud. The growing mantra of working from anywhere, at any time, utilizing any device—and bringing supply chains into the fold—also potentially brings global complications into the equation. Thus the perfect storm exposure.

Without paying equal attention to the risk associated with each of these trends, organizations could suffer tremendously. For instance, if a hacker got hold of an unprotected mobile device with complete access to the company's database and cloud investments, the potential for damage could permanently cripple an organization.

"This entire issue is driven from the top down. Leadership wants people within the business to have access to critical information to make a sale, service a customer or rapidly make decisions," explains Fergot. "Unfortunately, this means IT is playing catch-up. Even though they are typically the party who truly understands what is at stake, they no longer have complete control."

Protecting the organization against this potential perfect storm means IT leaders need to infuse themselves into the decision-making process around insurance coverage. "While this has traditionally been an area handled by the CFO, it is time for CIOs to take their seat at the table to provide a complete picture and ensure proper risk management and coverage," says Fergot.

So many risks are now moved into areas where the business has exposure that goes beyond traditional insurance coverage, explains Charron. "Standard insurance policies do not cover security and privacy, nor do they cover business interruption as a result of the cloud complication or the various activities now commonplace on mobile devices," he says. "These are specialty insurance offerings. And, if you aren't looking at it with an understanding of exactly what you need, then you most likely do not have the right coverage." ■