Cyber Risk in 2012:
Get Your Head in the Cloud

Cloud computing and other emerging technology exposures exacerbate the challenge of insuring and managing information security and privacy risks

By John W. DeWitt

Technology and information system innovations continue their relentless pace — putting cyber risk, data security, privacy, and related issues at the top of the 2012 concerns list for insurers, risk managers, chief information officers, and others who must grapple with the disruption and emerging risks created by each new entry to the technology marketplace. One of the most significant technology arrivals — not brand new, but exploding into an estimated $150 billion market by next year — is now ubiquitously referred to as "the cloud."

The metaphor of "the cloud" sounds mysterious, but it simply means that users increasingly are storing data off-site, accessing remotely hosted software applications, and relying on information technology infrastructure that is no longer on their physical premises. Instead, data, applications, and systems are "somewhere out there" (frequently, many places out there) and are accessed via the Internet from end users' businesses, homes, and mobile devices.

Everyone is in the cloud now — or at least impacted by it.

"Your company eventually will be interacting with someone in the cloud, whether or not you choose to go there," according to Hemanshu Nigam, founder of technology security advisory firm SSP Blue. "You used to be protected if you were in a 'small pond,' but now thanks to the Internet and the cloud, your small pond is connected to other ponds large, small, and in between, located all around the world."

Nigam — a former federal cybercrime prosecutor and advisor to the White House on cyber stalking, who has held top information security positions at News Corporation, Microsoft, and the Motion Picture Association of America — recently joined three other experts from Zurich for an in-depth PropertyCasualty360.com web seminar on the cloud and other current cyber risks. Through their presentations and answers to audience questions, Nigam and the other panelists explored a range of cyber- and information-related challenges and how to address them, including:

- The latest developments in cyber risk and how to gauge exposure—qualitatively and quantitatively
- How insurers and risk management experts are responding to an ever-changing risk landscape that impacts all technology users
- Practical and cost-effective approaches to manage and insure risk, including typical policy coverage and how to identify the elements that warrant coverage

The Ubiquity of Cybercrime and Information Security Risks

Nigam kicked off the discussion with sobering statistics on cybercrime: "Every day there are twice as many cybercrime victims as newborn babies," he said, adding that one in four Internet users (245 million in the U.S. alone) is a cybercrime victim. Businesses lose more than $130 billion annually — and are spending in the U.S. more than $75 billion a year on IT security. He then put this in the context of the cloud — used by one in every three business organizations in the U.S. today, and growing almost exponentially.

The good news is that "with everyone getting into the cloud, the risks can be identified and addressed," Nigam continued, citing reliability, information security and data breaches, bandwidth costs, and vendor lock-in as key concerns that businesses should have about the cloud. In addition to insurance and specific risk management approaches, Nigam emphasized the importance of choosing what he has dubbed "CIA vendors" — meaning those cloud technology providers that offer "confidentiality, integrity, and availability." Nigam also warned against focusing narrowly on cloud or any other risks, saying that a holistic point of view is required to protect organizations from diverse potential threats to information safety, security, and privacy.

"With everyone getting into the cloud, the risks can be identified and addressed."

Hemanshu Nigam

Former federal cybercrime prosecutor

Security and Privacy Risks Rival Traditional P&C Exposures

Adding further detail to the picture Nigam painted, the three Zurich experts made it clear that information security, privacy threats, and cyber-related exposures should be perceived and addressed with the same level of concern as traditional property and casualty exposures. Gregg Fergot, vice president and head of technology underwriting at Zurich North America, kicked off an in-depth discussion on the risk management strategies and insurance coverage needed to protect companies' information, intellectual assets, and reputation.

Most companies of any significant size have already "done the basics"—putting in firewalls, encrypting data, and maintaining up-to-date information security protocols — to protect their information-related assets, noted Larry Collins, vice president for HSE risk engineering and e-solutions at Zurich Services Corp. The question is how to go beyond this and actually anticipate risks that potentially face the business from all quarters.

As an illustrative example, Collins cited the "Night Dragon" attacks on oil and gas companies in 2009, noting that these were carefully targeted rather than random malicious efforts. "The attackers were trying to figure out how to underbid competitors to ensure they would win contracts when the went into competition with these energy companies," he explained.

In addition to technology-based corporate espionage, Collins also flagged increasing incidents of what's been dubbed "cyber hacktivism" — recruiting and mobilizing large numbers of participants who non-violently use "illegal or legally ambiguous digital tools in pursuit of political ends." Furthermore, cloud hacking — known as "hyperjacking"— has emerged with the rapid growth of cloud computing; similarly, the proliferation of powerful mobile devices such as smart phones, laptops and tablet computers has spawned malicious efforts to hack into these mobile devices.

To systematically mitigate a diversity of risks, Collins recommended "a scenario-based process to understand your exposures and to identify vulnerabilities." In this process, hazards are identified and assessed, their risk profiles ranked, and risk improvement actions put in place to address these with the appropriate prioritization. Expect this process to involve robust discussion and diverging viewpoints, he warned; the effort just to "create a simple chart to categorize acceptable and unacceptable risks" can result in "a heated conversation with your team."

Financial Impact, Risk Transfer, and Coverage Considerations

Data breaches and other cyber losses have many costs that are at least partially transferrable, noted Tim Stapleton, CIPP/US, who is assistant vice president and professional liability product manager at Zurich North America. Looking at a data breach example, an insured's transferrable costs can include direct expenses associated with crisis and reputation management, forensics investigation costs, the costs associated with notification to customers or others impacted by the breach, and business interruption costs. Third-party liabilities involved with some data breaches can include regulatory fines and penalties as well as legal liability, Stapleton added.

When it comes to data breaches and other losses associated with the cloud, companies need to be careful to protect themselves and not rely solely on vendors, said Stapleton.

"The reality is that most cloud providers cannot afford to indemnify everybody for losses," he said.

To ensure adequate insurance cover for a diversity of potential cyber and information-security losses, Stapleton pointed webinar attendees to three key areas: errors and omissions policies (which cloud providers often purchase for basic coverage), security and privacy liability coverage, and vendor services such as immediate support in the case of a breach.

"In many cases, adequate coverage can reduce the blow to the balance sheet and cover a good portion of transferrable costs," Stapleton said, adding that "no two E&O or security and privacy policies are alike — so be sure to compare each one to check for crucial elements" that apply to your particular business exposures.

ZURICH®