TOLMAN & WIKER
INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™
VENTURA | LOS ANGELES | SALINAS | SANTA MARIA | BAKERSFIELD

Cloud Computing: Risk vs. Reward

February, 2014

Property Casualty 360

Information technology professionals have recommended backing up files to protect information against hard drive crashes or stolen equipment since the integration of computers into the business world. Over the last three decades, data storage has evolved from floppy disks that held 1.44 megabytes of information to external storage capable of storing millions of megabytes (or, more concisely, multiple terabytes) of information.

Over the last few years, having enough storage space has become less of an issue, and the focus has shifted to accessibility. The newest tool to store data is the cloud, which gives users access to large amounts of storage space and makes that data available from any location and on many different devices. But although it has changed how countless professionals do business by being accessible from anywhere with an Internet connection, the cloud presents a new wave of cybercrime and hacking risks that businesses and their employees must protect against.

The concept of the cloud dates back to the 1950s, when a practice evolved that allowed multiple users of large and costly mainframes to share both physical access to the computer from multiple terminals as well as the CPU, or process time. That eliminated periods of inactivity on the mainframe and allowed for a greater return on investment. Today, a businesses can choose to deploy:

- A private cloud that it or a service provider owns
- A public cloud owned by a service provider
- A community cloud to be shared by multiple organizations, or
- A hybrid cloud that combines the former three options in some way.

Regardless of configuration, increased productivity is one of the most tangible benefits of the cloud. In a May 2013 Forbes Insight survey of more than 500 executives, 64 percent of respondents said that cloud-based collaboration tools translate into shorter time to market, quicker product upgrade cycles, and faster responses to competitive challenges. Companies also cited portable access to files, decreased expense, and greater scalability as advantages to using cloud services.

How the Cloud Can Work Against Business

With those benefits, why do some businesses still resist integration into the cloud? The biggest concern is the impact the cloud has on a company's security. With the ability to access anything from anywhere, a business's data can be more vulnerable to attacks. Cybercriminals are hard at work attempting to access data that now exists online, which previously only existed on a network accessible exclusively from firm offices. The logic mirrors the urban legend about 20th century bank robber Willie Sutton, who said he robbed banks because "that's where the money is." Cloud providers store data for many companies and individual consumers, making them a richer target.

The threat of exfiltration of corporate data by disgruntled employees is potentially even more worrisome. Freely available cloud storage tools make it possible for employees to remove any data from secured corporate networks that they may have access to and store it for retrieval on their personal devices.

Nearly three in four respondents in an IDC IT Cloud Services User Survey cited security as a concern for cloud adoption, making it the top concern. But although the consequences of a network or online data breach may keep executives up at night, the *likelihood* of a breach with information stored at a cloud provider may be a greater cause of concern.

Security concerns are generally more obvious in the cloud and include unauthorized access to sensitive data, potential lack of encryption both in transit and at rest, and the increased chance of the loss of data. What is typically

less considered by cloud storage users is the effect on data privacy. Contracts, data type, or the law may limit the use of third-party cloud storage providers to store information. Many regulations impact data storage depending on where the data originated and that strictly define where and how data may be stored.

Regardless of the service delivery model used by the cloud provider—for example, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), or even monitoring as a service (MaaS), communication as a service (CaaS), and anything as a service (XaaS)— the security responsibility can vary between the service provider and the customer.

And whether data is stored on a corporate network or the cloud, the impact a breach can have on a company extends from reputation issues to lost revenue and even legal action. Depending on the size and extent of a data breach, the data breach notification and network forensics costs alone can quickly escalate into hundreds of thousands of dollars or more.

Protecting Against Cloud-Based Risks

The 451 Research group, a global analyst and data company focused on enterprise IT innovation, projects that enterprise cloud computing will continue to grow 36% through 2016.

Although it seems as if many cloud providers rushed to market in spite of the risks associated with cyber security, the maturation of the market means many providers are now touting security as a feature. This helps ensure the encryption and protection from unauthorized access of data stored in the cloud.

Businesses considering cloud-based services should examine and understand the storage provider's systems, policies, and procedures, and to take their own existing contracts, regulations, and other risks into account. Corporate risk appetites differ, but with proper security and privacy controls in place, it's possible to minimize the potential threats. Securing data in the cloud needs to be the top priority for both the provider and the consumer (whether a business or individual) of the cloud.

Businesses using cloud service providers for data storage should recognize that it may increase the potential for loss. For example, a business that has data stored in multiple locations on one or more servers could increase risk by centralizing that data into one location. Likewise, a business may face a greater potential loss of control of sensitive data—personally identifiable information (PII), protected health information (PHI) or its own corporate intellectual property—if it chooses to store the data in the cloud.

Regardless of security, businesses today must operate with the mindset that a breach will happen and protect their financial and reputational interests through a cyber insurance policy. The policies generally provide first- and third-party coverage for data-breach-related exposures, which can include expenses incurred to notify affected parties of the breach and the cost to restore a business's reputation, in addition to addressing potential liability for a data breach. Coverage for forensic investigation, notification costs, and expenses incurred to hire public relations firms, establish call centers, and implement credit monitoring services commonly fall under cyber insurance policies. When unauthorized access to PII and/or PHI engenders regulatory fines and penalties, cyber insurance policies generally cover defense costs for regulatory proceedings. Some policies also extend coverage to assessed fines and penalties.

Cyber liability insurance presents a tremendous growth opportunity for insurance agents. To date, the take-up rate of cyber insurance has been relatively modest, with less than a third of businesses having purchased some form of cyber coverage. The year ahead may well prove to be the tipping point for recognizing the need for and purchasing insurance to address cyber-related exposures, including those exposures resulting from the use of cloud computing.

The cloud is a growing technology that evolves every day. While it can deliver significant bottom line benefits for many companies, growing cyber theft concerns require commensurate action. Businesses must implement appropriate tools and processes to prevent security and privacy breaches and choose a cyber insurance policy to protect themselves should a breach still occur.

Return to Article Index

Forward this article to a colleague

Address To Recipient Name


Subject
Message
Send
Reset