Every Silver Cloud Has a Dark Lining: A Primer on Cloud Computing, Regulatory and Data Security Risk

Carl Cadregari, CISA
is principal and practice lead in the Enterprise Risk Management Division of the Bonadio Group and also serves as chief information security director at one of the largest insurance companies in upstate New York (USA). Cadregari has more than 28 years of experience in IT and IS security architecture, deployment, project management, security by design and governance.

Alfonzo Cutaia, Esq., is an associate in the Information Technology & Internet Law Practice Group of Hodgson Russ LLP and focuses on patent practice. Before joining Hodgson Russ, Cutaia served as an intellectual property assistant for the Office of Science, Technology Transfer and Economic Outreach at the University at Buffalo (USA).

In the ever-changing economic and regulatory climate, business needs can change as rapidly as the weather. Organizations need to be agile so that they can adapt to the storms on the horizon. Budgetary constraints and increased regulatory compliance initiatives have forced organizations to look at alternative solutions to their everyday needs.

One such alternative: cloud computing.

But, how does using the cloud impact business? How would an enterprise survive the loss of highly sensitive business and client information in the cloud and the potentially resulting fines, sanctions and lawsuits?

“Cloud computing” is a term that many have come across recently and that is sure to confuse. “Cloud” is a term borrowed by IT organizations from the telecommunication industry of the 1990s. It is more of a broad concept than an exact science. Cloud computing, in its broadest meaning and in theory, is the mass centralization of computing resources. Through this centralization, information, processing and software are made available to a multitude of companies, users and services by tapping into this normally remote, independently controlled cloud. Through the use of new technologies, including virtualization, new computer resources can be provisioned quickly by organizations that need additional resources.

Ironically, centralized computing was the original computing model—a centrally located mainframe computer provided processing power, while lower-power “dumb terminals” were connected to the mainframe from remote locations. Over time, as processing power became less expensive, the computing model moved to a client-server model, in which a local set of servers performed basic functions (e.g., file storage, print queue management), and the majority of computing power that existed at the edge of the network moved within laptops and desktop computers. Now, with the ubiquity of the Internet, the availability of previously unattainable data transfer speeds and the affordability of bandwidth, moving data and processing needs to relatively inexpensive and powerful computers at a cloud provider shows the return to a more centralized computing model.

Although cloud computing, as such, is still in its infancy, several cloud concepts have been in wide use. The business of data processing has grown accustomed to cloud computing terms and concepts such as application hosting, including Software as a Service (SaaS) and application service providers (ASP); storage virtualization, including cloud storage and online backup; IT outsourcing (ITO); and business process outsourcing (BPO), including help desks, virtual data centers and hosted (platform) data centers. However, despite this familiarity, the potential for harm from centralizing and sharing resources has grown to a level that can quickly exceed the business case for cloud computing. This risk must be understood by every organization contemplating the use of a cloud solution so that the organization succeeds, or even thrives, through its efforts.

THE SILVER CLOUD—MEASURABLE SAVINGS
The benefits of using cloud computing are numerous. The shared nature and large scale of a cloud provider allow clients to quickly and easily scale their systems up or down to meet changing demands. This reduces the inefficiencies of traditional client-server deployments in which designers often overdesign capacity to ensure acceptable performance at peak demand. Also, many cloud-based systems enable users to access information from any web browser, even the latest smartphone and tablet platforms, and each user’s consumption of resources can be monitored to maximize the efficiency of the system.

Enterprises that deploy cloud-based systems can avoid capital expenditures on hardware and capitalized software. Small enterprises may also benefit from the economies of scale of a cloud provider that is able to leverage

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
expensive resources—such as system administrators, backup infrastructure and network infrastructure—across multiple clients. All of these areas can ostensibly lower the barriers to entry because infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks.

**THE DARK LINING OF THE CLOUD**

The benefits of cloud computing are tempered by the extreme potential to introduce uncontrolled or unforeseen risks and threats to an organization’s information. Enterprises must fully assess, understand and mitigate all risks before moving data into the cloud.

The information needed to run a business is a valuable asset—sometimes tangible, sometimes not. What are its own data and information worth to an enterprise? How much would they be worth to a cybercriminal? What could a hacker do with the information? What would it cost the enterprise if another company accidentally accessed and changed the data? What would the enterprise do if it lost its information, or access to it, due to a disaster at the cloud provider? How would the enterprise know if someone changed the data? What is an enterprise mandated by law to do if its data were exposed?

Security vulnerabilities and data loss incidents are a regular occurrence. In 2010, according to DataBreaches.net, the US Federal Bureau of Investigation (FBI), the Computer Security Institute (CSI) and multiple other organizations that track these incidents, there were hundreds of major incidents reported that encompass hundreds of millions of records—and those are just the reported ones. The reality is that one cannot open a newspaper or read an online article without realizing that cybercrimes and cybercriminals are a fact of life—just ask ALDI, T.J.Maxx, Heartland Payment Systems, the US Veterans Administration, Ben & Jerry’s, and PETCO, to name a few. The bottom line is that using a cloud provider can significantly increase the risk of a security incident and can increase all the costs, legal remedies and other losses that follow such a breach. However, in addition to the increased risk of an event, the costs of determining what happened and recovering from the event may be compounded by the abstract nature of cloud computing itself.

Data, and access to them, have real value to the continued operations of an enterprise and especially to the clients it serves. At times, most assuredly, data are valuable enough for someone, some enterprise or even some country to want to steal, manipulate or otherwise compromise the information. How much the data are worth to a cybercriminal directly translates into an enterprise’s threat posture. Attackers weigh their risks against their reward for getting that information.

When using the cloud, the question becomes: What does centralizing data with the data of dozens or hundreds of other enterprises do to an enterprise’s threat posture? The simple fact is that a business with data in the cloud has absolutely no direct control over where those data actually live. Also, standard service level agreements (SLAs) do not help much—cloud providers may do little, if anything, to ensure security, availability or response times for their clients. Most SLAs leave large time window carve-outs and best-effort hedges that do not provide concrete guarantees for business owners, especially as to their responsibilities under laws and regulations. Any time cloud computing is undertaken, data need to be reviewed, and at least the following six core questions from the Cloud Security Alliance need to be answered and defined:

1. How would the enterprise be harmed if the asset became widely public and widely distributed?
2. How would the enterprise be harmed if an employee of the cloud provider accessed the asset?
3. How would the enterprise be harmed if the process or function were manipulated by an outsider?
4. How would the enterprise be harmed if the process or function failed to provide expected results?
5. How would the enterprise be harmed if the information/data were unexpectedly changed?
6. How would the enterprise be harmed if the asset were unavailable for a period of time?

REGULATORY COMPLIANCE IN THE CLOUD

To maintain compliance with the US Federal Information Security Management Act (FISMA); the US Health Insurance Portability and Accountability Act (HIPAA); the US Health Information Technology for Economic and Clinical Health (HITECH) Act; the US Gramm-Leach-Bliley Act (GLBA); the PCI Data Security Standard (PCI DSS); the US Family Educational Rights and Privacy Act (FERPA); the US Children’s Internet Protection Act (CIPA); the US Sarbanes-Oxley Act; the 201 Code of Massachusetts Regulations (CMR) 17.00 (USA); California Senate Bill (SB) 1386 (USA); New York Information Security Breach Notification Act (NYISBNA) (USA); the US Code of Federal Regulations Title 21, part 11 (21CFR11); and other data security regulations, enterprises must have auditable requirements and actions. Therefore, enterprises need a thorough understanding of how using cloud computing affects their responsibilities and compliance actions. Generally, most laws and regulations require that an enterprise proves that its cloud provider (or ASP, SaaS provider and/or outsourcing host) has at least the same or similar controls in place as the enterprise’s internally hosted systems to protect the data per the law or regulation affecting it. So, if an organization is a public company that relies on a cloud-based, third-party payment processor that also has collections responsibility and receives personally identifiable information (PII) from the organization, what does that cloud provider have to do? What does the enterprise have to do, and what happens when data are lost, inappropriately accessed or otherwise compromised?

COST OF A DATA BREACH

In today’s world, misappropriated data, stolen and lost physical assets, and unintentional and intentional breaches occur with frightening regularity to every type and size of business. The recent study done by the Ponemon Institute regarding the cost and frequency of cybercrimes shows that the companies surveyed each had at least one successful cybercrime per week and that the annual cost of managing those attacks exceeds US $5.8 million. The study details costs in most affected business areas, including cybercrime detection, avoidance, incident management and asset loss, but does not include noncompliance fines, sanctions and lawsuits that could easily double the true costs. Some recent fines levied include:

• Rite Aid®—US $1 million for a HIPAA violation
• The TJX Companies Inc. (of which T.J. Maxx is a part)—US $40.9 million for lost credit card data
• Health Net of NE—US $250,000 for a lost hard drive
• Six California (USA) hospitals—More than US $790,000 by the California Department of Public Health (CDPH) for a privacy data breach

As cloud computing grows, so will its exposure and use in criminal activity, as will the need for cloud forensics. This is evident in any recent data breach headline or on any data breach web site. For example, Cloutage.org (founded by the Open Security Foundation) stated that, in 2010, of the 322 incidents reported, 54 incidents of identified data loss occurred because the cloud provider was hacked or because a cloud vulnerability was found.

ASSURING THE CLOUD

The use of cloud resources can be highly beneficial to most enterprises—but one should always know the risks, use the appropriate resources and experts from the audit and legal community, and be prepared to answer the following questions:

• Security:
  – How are data encrypted at rest and in transit?
  – How are data protected from unauthorized access?
  – How are data disposed?
  – How is cloud provider internal security handled?
    · Administrative controls
    · Physical controls
    · Logical controls
  – What rights and abilities does the enterprise have in the case of a breach (e.g., right to audit, ability to perform forensics investigations)?
  – What reporting obligations does the provider have to notify users of security breaches (e.g., indemnification for breaches)?
– What actions has the provider taken to prevent attacks?
– What protections does the provider require the enterprise to have in place?
– How does the provider reliably demonstrate and communicate its security procedures to its clients?
– How much ability does the provider give its consumers to perform their own assurance procedures, such as security scanning or audits?
– How does the provider handle overlapping or contradictory interstate regulations on data privacy?

**Compliance:**
– What compliance standards does the provider meet?
– How will compliance be maintained before, during and after a move to the cloud?
– What third-party assurance (e.g., SAS 70, WebTrust, SysTrust, etc.) documentation is in place that assures compliance?
– How can the enterprise track the physical location of its data for compliance (e.g., certain laws prevent data from being stored in certain countries)?
– Beyond just data security, what documentation will be provided to the enterprise that will allow it to maintain compliance requirements with legislation such as the US Sarbanes-Oxley Act?
– Is the enterprise prepared to maintain the needed internal controls and compliance to the levels required by all of its data?
– At what point is too much information regarding internal controls and procedures being provided by the enterprise, thereby endangering the business?

**Availability:**
– How much uptime is guaranteed?
– Is there a guaranteed service level? Who monitors it? What reimbursements will occur if the guaranteed level is not met?
– Now that all services are accessed over the Internet, does the enterprise have enough bandwidth for all of its employees, and/or does the provider have enough power and bandwidth to service the enterprise’s needs?
– Can service be interrupted based on the activity of nonrelated cloud consumers (e.g., a hard drive subpoena)?
– How is information segregated between clients?
– How will assurance be provided by the cloud provider with regard to availability?
– To what level is the cloud provider responsible, fiscally, legally or otherwise, for lost business as a result of service outages or issues?
– What are the disaster recovery and business continuity plans once the enterprise has a cloud infrastructure?

**Operations:**
– How can the enterprise monitor the load and performance of the cloud?
– How can the cloud provider assure the enterprise that it is being billed fairly for usage?
– What tools are available and allowed to monitor security in the cloud?

** Entire project:**
– Who is the independent auditor for all the previously mentioned areas?
– How often are the audits performed?
These questions are the most basic that should be answered when contemplating the use of a cloud provider; enterprises should be prepared to have in-depth technological, legal and business conversations on each. In all cases, an unsure or negative answer from the cloud computing vendor should be considered a deal breaker because even one poor control could be used to exploit all of an enterprise’s data.

**CONCLUSION**
As cloud computing continues to push into the mainstream of information processing, data storage and cross-border communication, it is critical that the risks to data are consistently reviewed and that the threats identified are mitigated to a level commensurate with the value of the data. The value of a cloud computing infrastructure is measurable: savings can be achieved in data accessibility, customer relationship management, and decreased hardware costs and infrastructure support, but the costs of a breach or of lost data can easily outstrip any savings with the potential regulatory agency fines, civil lawsuits and reputational damage. Remember that it is always the enterprise’s responsibility to keep its data confidential, maintain their integrity, assure their availability, meet its obligations under regulations and laws, and not get lost in the clouds.
ENDNOTES


14 Op cit. Jewell, Mark

