July 30, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

The Cloud, Cyber Security, and Cloud Cyber Governance:
What Every Director Needs to Know

*By Paul A. Ferrillo, Dave Burg, and Aaron Philipp**

There are four competing business propositions affecting most American businesses today. Think of them as four freight trains on different tracks headed for a four-way stop signal at fiber optic speed.

First, with a significant potential for cost savings, American business has adopted cloud computing as an efficient and effective way to manage countless bytes of data from remote locations at costs that would be unheard of if they were forced to store their data on hard servers. According to one report, "In September 2013, International Data Corporation predicted that, between 2013 and 2017, spending on pubic IT cloud computing will experience a compound annual growth of 23.5%."[1] Another report noted, "By 2014, cloud computing is expected to become a $150 billion industry. And for good reason – whether users are on a desktop computer or mobile device, the cloud provides instant access to data anytime, anywhere there is an Internet connection."[2]

The second freight train is data security. Making your enterprise's information easier for you to access and analyze also potentially makes it easier for others to do, too. 2013 and 2014 have been the years of "the big data breach," with millions of personal data and information records stolen by hackers. Respondents to the 2014 Global State of Information Security® Survey reported a 25% increase in detected security incidents over 2012 and a 45% increase compared to 2011.[3] Though larger breaches at global retailers are extremely well known, what is less known is that cloud providers are not immune from attack. Witness the cyber breach against a file sharing cloud provider that was perpetrated by lax password security and which caused a spam attack on its customers. "The message is that cyber criminals, just like legitimate companies, are seeing the "business benefits" of cloud services. Thus, they're signing up for accounts and reaching sensitive files through these accounts. For the cyber criminals this only takes a run-of-the-mill knowledge level … This is the next step in a new trend … and it will only continue."[4]

The third freight train is the plaintiff's litigation bar. Following cyber breach after cyber breach, they are viewing the corporate horizon as rich with opportunities to sue previously unsuspecting companies caught in the middle of a cyber disaster, with no clear way out. They see companies scrambling to

* Paul Ferrillo is counsel in the Securities Litigation practice at Weil, Gotshal & Manges LLP. Dave Burg is a Principal and Global & U.S. Advisory Cybersecurity Leader at PwC. Aaron Philipp is a Manager in the Advisory-Forensic practice at PwC.

contend with major breaches, investor relation delays, and loss of brand and reputation.

The last freight train running towards the intersection of cloud computing and data security is the topic of cyber governance – i.e., what directors should be doing or thinking about to protect their firm's most critical and valuable IP assets. In our previous article,[5] we noted that though directors are not supposed to be able to predict all potential issues when it comes to cyber security issues, they do have a basic fiduciary duty to oversee the risk management of the enterprise, which includes securing its intellectual property and trade secrets. The purpose of this article is to help directors and officers potentially avoid a freight train collision by helping the "cyber governance train" control the path and destiny of the company. We will discuss basic cloud security principles, and basic questions directors should ask when considering whether or not the data their management desires to run on a cloud-based architecture will be as safe from attack as possible. As usual when dealing with cyber security issues, there are no 100% foolproof answers. Even cloud experts disagree on cloud-based data security practices and their effectiveness.[6] There are only good questions a board can ask to make sure it is fulfilling its duties to shareholders to protect the company's valuable IP assets.

What is Cloud Computing/What Are Its Basic Platforms

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down to provide an on-demand utility-like model of allocation and consumption."[7]

Cloud computing is generally based upon three separate and distinct architectures that matter when considering the security of the data sitting in the particular cloud environment:

- Infrastructure as a Service (IaaS) – think of this as a basic foundation of all cloud-based services. It includes everything from the hardware facilities to the software that resides in them. All computer services under IaaS are fully outsourced. An IaaS user will need to manage several components. In addition to applications and data, this includes middleware, application run time and operating systems. The ability to manipulate data within the cloud comes with the downside that such data can be compromised.
- Platform as a Service (PaaS) – is the delivery of a computing platform and a solution stack as a service. It allows a buyer to deploy applications without the cost and complexity of buying and managing the underlying hardware and software.
- Software as a Service (SaaS) – is a self-contained, software delivery platform that sits above IaaS and PaaS, and delivers the entire user experience, including content and presentation. The SaaS vendor manages all aspects of service delivery, and client downloads and installations are kept to a minimum. The consumer doesn't generally manage any aspect of the infrastructure. In most cases, the SaaS vendor is also generally responsible for security.[8]

Now, if the above discussion of the types of cloud platforms isn't confusing enough, data security issues on the cloud are equally complicated. But they can be boiled down into several concepts that can be easily understood:

- **Data Migration to and from the Cloud** – Managing data is always a challenge in a highly developed organization. It gets even more interesting with the cloud and even further interesting with the advent of mobile devices. Cloud-based systems should be able to alert the consumer to situations where there is unapproved data moving to the cloud, and data moving within the cloud or to other cloud-based providers.
- **Geographic and Regulatory Considerations** – The type of information that is considered third

party or personally identifiable information varies greatly from world region to world region. Making sure that the data stays in the proper region and under the right regulatory regime and doesn't cross geographic boundaries in violation of the applicable laws is a primary concern in cloud.

- **Data Encryption** – Data is first encrypted (e.g., encoded) from the endpoint to the cloud so that it is not intercepted and stolen in transit. There are many types of encryption techniques available depending upon the type and volume of data stored.
- **Continuous Monitoring** – Probably one of the most important aspects of cloud security is the ability of the cloud-based provider to monitor in real time all database activity, across multiple database platforms.
- **Incident Response and Data Recovery** – A last key element of any cloud-based provider is its ability to quickly respond to an incident and provide instant notification to the consumer that an attack has been attempted. Additionally, any cloud-based provider should have a ready-to-go, battled tested, disaster data recovery plan.

We note that there are highly secure cloud providers that employ cutting edge security architecture as well as cybersecurity analytic capability that may make future risk decisions related to migrating the cloud not only more efficient, but more cost effective with reduced (not increased) risk.

Cloud Cyber Governance

As shown above, what is commonly referred to as the cloud actually can mean many different things depending on the context and use. Using SaaS to manage a customer base has a vastly different set of governance criteria to using IaaS as a development environment. As such, there are very few accepted standards for properly monitoring/administering a cloud-based environment. There are many IT consultants in the cloud-based computing environment that can be consulted in that regard. Our view, however, is that directors are ultimately responsible for enterprise risk management, and that includes cyber security, a subset of which is cloud-based cyber-security. Thus it is important for directors to have a basic understanding of the risks involved in cloud-based data storage systems, and with cloud-based storage providers. Below are a few basic questions that come to mind that a director could pose to management, and the company's CISO and CIO:

1. Where will your data be stored geographically (which may determine which laws apply to the protection of the company's data), and in what data centers?
2. Is there any type of customer data co-mingling that could potentially expose the company data to competitors or other parties?
3. What sort of encryption does the cloud-based provider use?
4. What is the vendor's backup and disaster recovery plan?
5. What is the vendor's incident response and notification plan?[9]
6. What kind of access will you have to security information on your data stored in the cloud in the event the company needs to respond to a regulatory request or internal investigation?
7. How transparent is the cloud provider's own security posture? What sort of access can your company get to the cloud provider's data center and personnel to make sure it is receiving what it is paying for?
8. What is the cloud servicer's responsibility to update its security systems as technology and sophistication evolves?
9. What is the cloud provider's ability to timely detect (i.e., continuously monitor) and respond to a security incident, and what sort of logging information is kept in order to potentially detect anomalous activity?[10]
10. Are there any third party requirements (such as HITECH/HIPAA) that the provider needs to conform to for your industry?
11. Is the cloud service provider that is being considered already approved under the government's FedRamp authorization process,

which pre-approves cloud service providers and their security controls?[11]

12. Finally, does the company's cyber insurance liability policy cover cloud-based Losses assuming there is a breach and customer records are stolen or otherwise compromised?[12] This is a very important question to ask, especially if the company involved is going to use a cyber-insurance policy as a risk transfer mechanism. When in doubt, a knowledgeable cyber-insurance broker should be consulted to make sure cloud-based Losses are covered.

High-profile breaches have proven conclusively that cybersecurity is a board issue first and foremost. Being a board member is tough work. Board members have a lot on their plate, including, first and foremost, financial reporting issues. But as high-profile breaches have shown, major cyber breaches have almost the same effect as a high profile accounting problem or restatement. They cause havoc with investors, stock prices, vendors, branding, corporate reputation and consumers. Directors should be ready to ask tough questions regarding cyber security and cloud-based security issues so they do not find themselves on the wrong end of a major data breach, either on the ground or in the cloud.

This article was first published by The D&O Diary on July 29, 2014.

[1] *See* "Cloud Security Report – Spring 2014," AlertLogic, 2014.

[2] *See* "8 Reasons to Fear Cloud Computing," BusinessNewsDaily, October 2013.

[3] PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013.

[4] *See* "Cloud-based services emerge as potential platforms for cyber-attacks," Fedscoop, June 30, 2014.

[5] *See* "Guest Post: Cyber Security, Cyber Governance, and Cyber Insurance: What Every Public Company Director Needs to Know," D&O Diary, June 4, 2014.

[6] *See* "Data Breach: the Cloud Multiplier Effect," Ponemon Institute, June 2014.

[7] *See* "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, 2011.

[8] Note that regardless of the architecture framework, service level, security, governance and liability issues are normally address in a service level agreement (SLA) which is offered to the customer. Those should be thoroughly reviewed by legal counsel in additional to the CIO/CISO review of the particular cloud environment.

[9] Proper Security Incident Management is built upon knowledge of the tactics, technologies, principles, and processes to protect, analyze, prioritize, and handle incidents. *See* http://cloud.cio.gov/topics/security-incident-management.

[10] *See* NIST Special Publication 800-137 Continuing Monitoring Process.

[11] *See* here. The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[12] *See* "In Cloud We Trust Our Data: Can you Trust Your Cyber Insurance Policy?," Data Breach Insurance, May 30, 2014.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.