Cloud Computing in Education: Rewards & Risks

According to a 2012 Cisco and affiliates report, in the next five years, institutions of higher education expect to cut 20% of their IT budget by moving applications to the cloud. While the future of cloud computing in higher education settings is positive, there are still risks involved. Education organizations can model their approach to new cloud technology after the business sector, where similar risks apply. But no cloud solution should be one-size-fits-all.

Technology and Cloud Computing in Higher Education

2010 marked the first year in which more data traveled across the Internet than during all the previous years combined. As a result, about one-third of U.S. colleges and universities are developing strategic plans for the adoption of cloud computing, or are already in the process. This process of transferring data to the cloud will ultimately save institutions money: the average savings from migration applications to the cloud is 21 percent. Cloud computing becomes a low cost option for using high concept computing systems. Additionally, because confidential and critical data can be stored centrally in the cloud, there is less exposure to threats of saved data; the top use of the cloud is storage, with 31 percent of it used in higher education, and 40 percent used in K-12 education.

Over half of the educational institutions want increased efficiency and believe cloud computing is the answer because it saves money and resources. Additionally, the use of mobile technology in schools allows for easy access to the cloud. Already one-third of elementary, middle and high school students say they use their iPad for schoolwork, while 44 percent say they use their smartphone. However, it is important to remember that even though money can be saved by switching to a cloud based system, offering the ability to work outside of the classroom may increase the risk of information loss or enable student-to-student cheating.

Taking some simple steps can help minimize this risk. Incorporating privacy policies that mandate the use of screen privacy products, such as 3M™ Privacy Filters and Screen Protectors, on all school-issued devices can help prevent this disclosure of information, along with the “recommended remediation for cloud security risks” to the right, and the following others:

The Three Biggest Risks of Cloud Computing

While cloud computing has been around for a few years, widespread corporate use is growing at an incredible rate. According to Forrester Research, company spending on cloud computing services should rise from $58 billion in 2013 to $72 billion this year, with the market reaching $191 billion by 2020.
The 451 Group’s Market Monitor says spending on cloud computing is growing at an annual rate of 24 percent. However, while there are many benefits for companies to move their data to the cloud, the risks the service poses to organizations need to be addressed before complete, system-wide adoption.

**Limited Employee Controls**

Employees are often seen as the weak link in the chain of security. While the cloud can be an efficient way for workers, educators and students to access critical information and be more productive, it also poses security challenges since they’re accessing this information wherever they are working, which includes the office, airplanes or coffee shops. This makes protecting sensitive corporate data an even bigger hurdle for organizations than ever before. With the push towards consumerization in organizations, leaders don’t always have control on what device this information is being accessed from. It’s important for organizations to introduce the proper security controls, including educating staffers on the proper encryption methods to upload data securely into the cloud, mandating the use of privacy screen protectors for devices when downloading information in public, and consenting what information can be authorized where and by whom.

**Limited Understanding of EULA Agreements**

The small print of the end user license agreement (EULA) for cloud service providers may contain information that completely indemnifies the provider from any and all wrongdoing and liability. All liability, accountability and responsibility for site usage are assigned to the user through the EULA. The corporate entity has no recourse to recover data or learn of incidents based upon legal wording and requirements in the EULA. In most cases, the EULA provides the user a “take it or leave it” option of using the service stating no fault clauses that fully protect the vendor. Organizations are left with the option of not using the service at all, or using the service assuming all risks as if the service was offered as an internal company product.

**Unknown Cloud Supply Chain**

This can sometimes be called the “known unknowns” of cloud computing. Corporate users know they are storing information in the cloud through the defined provider, however, they really do not know where the data is physically being stored or who may have access to their data.

Cloud service users may assume it is a single company providing end-to-end service. The reality is that most cloud providers do not run a homogenous labor environment. Nor may the cloud provider reveal physical or virtual access policies and procedures and the continued management of new hires and terminations. This can lead to advertent and inadvertent access to data and the loss of that data to malicious insiders and cyber criminals.

Furthermore, company data may be stored in multiple data centers throughout the United States or even in offshore locations. This will complicate any potential data recovery effort since the laws of another country may take precedence of those of the United States. Lastly, the fact that data may be stored offshore can lead to additional risk of malicious activity.

**Conclusion**

The three biggest risks of cloud computing can be controlled if common sense is used to protect what is stored in the cloud and how it is accessed. The critical threats to cloud usage require
just a little bit of thought, due care, and due diligence to ensure the private information is protected. Users help protect what others see through mobile devices and computer screens by incorporating screen privacy filters and conducting business outside the wandering eyes of others. Reviewing EULAs is a must to understanding user rights and limitations. As a rule of thumb, never post anything in the cloud that you would not want a stranger to know. Maintain the privacy of your information by practicing safe cloud computing.