Audit Tidbits

Cycle 2 Internal Control Assessment (ICA) training is scheduled for September 21st at 2:00 p.m. and October 19th at 2:00 p.m., in the Human Resources training room. To sign-up, please email auditing@olemiss.edu.

Cloud Storage and Sensitive Data

Effective July 1, 2011, Mississippi has a data breach notification law, House Bill 583 (see http://billstatus.ls.state.ms.us/documents/2010/html/HB/0500-0599/HB0583SG.htm). This law defines what data is considered to be sensitive (confidential), what constitutes a breach under this law, and the process that must be followed in the event sensitive information is “leaked” in a data breach. In addition to the state law description, the University also considers student grades, private correspondence, classified research, etc. as sensitive. The growing trend to store business, including university, data on a “cloud” has brought to the forefront data security issues and concerns.

Sites like Dropbox, Amazon, Google and countless others offer storage that can be accessed remotely from any device (desktop, laptop, smartphone, tablet, etc.) using the Internet. Users should note, however, that this convenience comes at a price – a price that can be too high when sensitive data is involved. Cloud-based services for storing data are very popular, mostly because of the easy, convenient access they provide. Often, this easy access is the driving factor for using cloud computing, and other critical concerns such as reliability, data security and liability are relegated to the background. This article focuses on the security, liability and reliability risks of cloud-based data storage services.
How Safe is Your Data in “the Cloud”? 

While larger, more reputable cloud storage companies have the money, resources, and technical expertise to address reliability and security, they often contain usage clauses that free them from any responsibility for “lost, stolen, or damaged data” or from unauthorized access to data. However, if you cause a person’s sensitive data to be compromised, you are responsible under Mississippi law. The University will be required to notify every individual whose data was exposed and may be subject to other penalties. Meanwhile, the cloud service itself will be insulated from the consequences of any breach by its usage agreement. This may prevent you and your organization from recouping any of the costs associated with the breach; it also reduces the service’s incentive to protect data as carefully as it should.

Data Breach Examples

Last month, Dropbox had a security issue in which password authentication was disabled for 4 hours. This means that any documents stored on their servers were susceptible to access without a password during this interval. For more details, see the Computer World article at the following Web address:
http://www.computerworld.com/s/article/9217799/Dropbox_left_document_storage_accounts_open_for_four_hours

The following Security News Daily article on May 4 of this year detailed a vulnerability in which Dropbox stores unencrypted login files on each device. In the event these login files were copied maliciously, the entire user’s account would be accessible without requiring any login credentials:
University Policy for Protecting Sensitive Data

UM’s Information Confidentiality/Security Policy (see http://secure4.olemiss.edu/umpolicyopen/ShowDetails.jsp?istatPara=1&policyObjidPara=10654991) addresses the requirements for protecting confidential data. It is never acceptable to store confidential data such as grades, social security numbers, private correspondence, classified research, etc. on externally hosted systems, including cloud-based storage systems, without a contract that is fully vetted for compliance with university policies.

Secure Document Exchange

Please keep in mind that confidential data should not be sent using email either. Likewise, do not store files that contain sensitive data on Web servers where they might be inadvertently accessed or indexed by search engines such as Google. The safest way to exchange sensitive or confidential information with other university employees is by using Secure Document Exchange within myOleMiss. To access Secure Document Exchange, point your Web browser to http://my.olemiss.edu, and choose Employee -> Tools and then Secure Document Exchange from the Detailed Navigation on the left.
Be Aware!

It is more important than ever to be aware of how you store and transmit confidential data. Your first choice should always be to store confidential data on university-owned, protected systems such as those housed in the Data Center and protected by a university firewall. If information must be stored at the department level or on your desktop or laptop computer, then the servers on which the data resides must be registered with IT so they can be scanned periodically for any security vulnerabilities. Occasionally, departments may have a need to use externally hosted systems that contain sensitive data. In this case, the contract for these services must address the requirements for protecting confidential data as defined in the UM’s Information Confidentiality/Security policy.

If you have any questions related to IT security please contact the IT Helpesk and they will work with your office to find solutions for protecting and storing sensitive or confidential data.

*We strongly encourage that at least one employee from each department attend an upcoming training session. If you have any questions, please feel free to contact us at 915-7017 or auditing@olemiss.edu.*