Cloud Computing Security: An Oxymoron?

EDUCAUSE 2010 Conference discussion session notes (under Resources tab) http://www.educause.edu/E2010/Program/DISC14

References mentioned by session participants:

Matthew Dalton http://www.educause.edu/Community/MemDir/Profiles/MatthewDalton/47982
  ● Ohio University - Security and Policies (click on Standards, then Outsourcing Technology) - http://www.ohio.edu/technology/security/

Maria Ebner-Smith http://www.educause.edu/Community/MemDir/Profiles/MariaEbnerSmith/96853

Jon Good http://www.educause.edu/Community/MemDir/Profiles/JonGood/41241

Tom Trappler http://www.educause.edu/Community/MemDir/Profiles/ThomasTrappler/47672

(Could someone please send me a reference to the resource mentioned from Central Piedmont Community College? - thanks!)

Discussion Session Notes:

  ● For the purposes of this session, we’re going to consider “cloud” to mean commercially available services such as Google Apps, Amazon EC2, Microsoft Live@EDU.
    ○ However, many of the cloud security issues/concerns found with commercially available services are also relevant to private and institutional/consortial clouds

  ● The speed of adoption of cloud services has accelerated - it’s now so easy to share information that people are more likely to make mistakes, that some have found that they need to find way to mitigate the ease of use of such services!

  ● How should treating security/privacy in the cloud be any different than how we treat locally sourced services? Existing policies that cover FERPA, HIPAA, etc., should cover the cloud as well.
    ○ Note that it’s difficult to terminate a person who violates policy, regardless of sourcing method.
• Do we *really* have more control if we run our services locally? In some cases, security may be higher for some cloud-based services than you can provide locally.
  ○ Perhaps the problem with accepting non-locally sourced services is emotional, and we need to address the emotional response.

• Who is responsible for a data breach if you’re utilizing a cloud service?
  ○ Need to address this issue through contracts with the cloud providers that establish shared liability.
  ○ Need to establish a level of trust.
  ○ May wish to consider designing services so that restricted data is only stored locally.

• Some campuses want control over any information that causes significant damage to the university.
  ○ What does this even mean? Does it include an indiscretion in the e-mail of a senior campus executive? How can you prevent release of information like that?

• How do you get information that is in the logs of a cloud-based service? Do you even know if the cloud provider is keeping logs and what information is collected in the logs?
  ○ Need to address this issue through contracts.

• Subcontractors used by cloud providers can be a problem.
  ○ Need to have the subcontractors complete the same contract that your cloud providers do.

• Consider “cyber risk insurance”
  ○ Oakland University requires $1M minimum insurance

• Data retention is a problem.
  ○ A cloud provider’s servers can be located anywhere internationally.
  ○ How can we recall information?
  ○ What about legal records retention issues with e-mail? Saving all e-mail forever isn’t an option, and isn’t advisable because of issues such as e-discovery.
    ■ If it’s a record that needs to be retained, the record creator needs to copy it to a location that isn’t e-mail.

• Does anyone know of a cloud service that scans anything uploaded for the presence of restricted data, i.e., DLP (data loss prevention) cloud service?
  ○ No, but others in the room are looking at locally hosted DLP products

• What about encryption of e-mail and data?
  ○ Need to determine the definition of encryption.
    ■ Is it an enterprise solution or a key escrow system?
  ○ End-user training is important for e-mail encryption.
• Is anyone concerned about increased possibility of corporate espionage when using cloud services?
  ○ Something to remember is that corporate espionage is not just a problem with cloud employees. Your own employees are likely to be a greater problem.

• Key point about security and privacy concerns - reputational damage to the institution is far worse than monetary damage.

Thanks to everyone who attended the session - I learned a lot from all of you, and I hope that you had at least one “take away” of value from the session!
- Melissa Woo http://www.educause.edu/Community/MemDir/Profiles/MelissaWoo/47525
  - last revised 16 Oct 10