THINGS YOU SHOULD KNOW ABOUT...
CLOUD SECURITY

Scenario

When a medical researcher at the university's teaching hospital won a federal grant to study new treatments for Alzheimer's patients, he requested a sophisticated computer system—unlike anything the IT department had previously implemented or supported—including both storage and application components. Although part of the grant could fund this system, Rachel, the institution's CIO, soon saw that obtaining these services from the cloud was a better option than developing them in-house. At the same time, though, the project raised several security questions that would need to be addressed. The research involved not only human subjects but also graduate students, and the institution had to ensure the privacy of those individuals. The research results were potentially extremely valuable to pharmaceutical companies, and the researcher demanded assurance that the data would be secure. In addition, because the project was funded by a government grant, the computer system had to provide reliable audit trails.

Rachel began with a list of cloud providers that could offer the storage and application processing that the researcher would need for the complex computations and huge data files. She asked her information security officer to work with the institutional risk manager to conduct a risk assessment of those providers, eliminating several vendors that were not sufficiently transparent regarding their security policies and procedures. She consulted resources developed by other colleges and universities on the security profiles of the cloud providers on her list, and she obtained proposals from four of them. Working with the researcher, Rachel then evaluated the institution's potential exposure and risk tolerance. None of the providers met all of the security requirements the institution needed, so Rachel approached the four companies and asked about making the needed changes to their contract terms. Two vendors were unwilling to deviate from standard terms, but the other two were open to customized agreements. After some negotiation, Rachel settled on one of these cloud providers to furnish the IT services the institution needed. The final decision came down to the provider whose policies allowed a greater level of institutional control over the data stored off-site and that had more robust procedures for backup and recovery of data. This vendor was also the one that had previous experience working with medical research teams and that had been recommended to Rachel by a colleague at another university.

educause.edu

1 What is it?

Many contend that cloud computing holds promise to provide considerable benefits for colleges and universities. By moving storage, processing, applications, or other IT infrastructure and services to the cloud, institutions might realize increased reliability and flexibility, with lower or more transparent costs. Even the most optimistic scenarios, however, must account for a raft of security questions that are complicated or exacerbated due to the loss of control. Information security depends on the three principles of confidentiality (who has access), integrity (correctness of information), and availability (ability to access information and services at appropriate times). These elements constitute computer security in any context, and they take on new significance in cloud computing because it depends on third-party providers. Higher education is subject to regulations concerning the protection of student records and other data, and individual campuses tend to be idiosyncratic with respect to state or local requirements and cultural attitudes towards risk. In this context, any institution that turns to cloud computing faces important questions about how information assets will be safeguarded and what measures are in place to secure those assets over time.

2 How does it work?

Cloud security involves the same fundamental issues as any computer security program: restricting access to authorized users, maintaining the integrity of data, and ensuring the availability of data and services. When data and services reside on servers external to the campus, however, safeguarding those assets involves additional concerns. Encrypting data in transit is important, as are the service provider's security procedures. Cloud computing typically uses server virtualization, and if the virtualization isn't secure, data from one segment of a server could "escape" into another area. Frequency and reliability of data backups are important, as is the recoverability of data in the event of a glitch or data loss. E-discovery is another consideration when data are not stored under direct institutional control. Institutions must rely on cloud providers to meet a certain level of availability, despite downtime for system maintenance, upgrades, or power outages. The long-term viability of the cloud provider is another aspect of availability—institutions should have contingency plans if a cloud provider goes out of business, merges with another company, or otherwise ceases to provide contracted services. Additional questions arise about which jurisdiction's laws apply in a dispute and about where data are stored—regulations might require that data be stored in the institution's home state or country. The service level agreements (SLAs) that cloud providers offer are often not sufficiently specific to meet the requirements of a college or university. Cloud customers would usually undertake a risk assessment of any third-party provider, and

more >>

EDUCAUSE
UNCOMMON THINKING
FOR THE COMMON GOOD

increasingly organizations such as Shared Assessments provide resources to assist in this effort.

3 Who’s doing it?

As growing numbers of organizations—including colleges and universities—turn to cloud computing, cloud providers are implementing new features and services to build confidence that cloud computing can provide appropriate levels of security assurance. In the past few years, companies have emerged that add a layer of security onto cloud services, and in some cases, cloud providers have acquired these companies and incorporated the technologies into their products and services. In 2009, the nonprofit organization Cloud Security Alliance was launched to provide information and resources about best practices in security for cloud computing, as well as to conduct research and engage in educational activities about cloud security. At institutions where concerns about cloud security cannot be addressed by commercial cloud providers, private clouds might be an alternative. Private clouds take advantage of the fundamental attributes of a cloud infrastructure, but they typically offer more control and restrict access to a limited pool of users. Private clouds offer greater ability for customization and control, allowing high-risk or idiosyncratic IT services to reap many of the benefits of public clouds. The operator of a private cloud is often one of the institutions using it, and because of the trust and common requirements within a consortium of users, private clouds can often address many cloud security concerns.

4 Why is it significant?

Advocates of cloud computing promise great things, and many believe that the claims are not merely hype—that cloud services will be a defining characteristic of the next era of computing. Security could be the cloud’s Achilles’ heel, however, and must be sorted out for cloud computing to reach its potential. Information systems cover a spectrum of requirements—from total protection to complete openness—and internal risk assessments are the means by which an organization evaluates the trade-offs and decides what level of security is acceptable and appropriate. Cloud computing not only adds new layers to the question of computer security, it often also adds complexity in understanding the parameters that feed into a risk assessment. Because the systems and staff of a cloud provider are not under the control of a customer, institutions that use cloud services rely on contracts—and, to be sure, a certain amount of trust—for security information. Vendors offer different levels of transparency, and this becomes an important component of institutional efforts to evaluate cloud services.

5 What are the downsides?

Measures taken to enhance the protection of information assets tend to work against access to information. To the extent that security considerations are more complex in a cloud environment, the likelihood rises that users of those IT services will see decreased flexibility. In some cases, the security concerns confronting cloud computing are novel, and many vendors lack experience with such issues. Until replicable best practices emerge, the time and expense required to effectively mitigate the security risks of cloud computing will offset some of the benefits that it offers. Moreover, although the cloud provider is responsible for maintaining data and services, legal liability for those assets—as well as the responsibility to notify users in the event of a breach—typically remain with the college or university.

6 Where is it going?

Colleges and universities have deep concerns about the loss of control in cloud computing, and concern about security is one of the factors limiting greater adoption. Contract terms, liability provisions, indemnification, and exit strategies are vital. To this end, the Higher Education Information Security Council maintains a toolkit called Data Protection Contractual Language designed to provide sample language and guidance to institutions exploring cloud computing and similar services. Cloud providers might need to be more transparent with their processes and will perhaps move toward SLAs that are acceptable to larger numbers of colleges and universities. At the same time, private clouds will evolve to meet the needs of institutions with unique or more stringent security requirements. Institutions will also explore the security implications for integrating cloud services with those hosted on campus.

7 What are the implications for higher education?

Regulations such as HIPAA and FERPA and expectations about the role higher education serves for students place a premium on institutions’ ability to understand the risks of IT services and systems and make appropriate determinations about risk tolerance. Some cloud providers, for instance, might mine data for marketing purposes. At the same time, cloud services might provide *greater* security than an individual campus could achieve on its own. Meanwhile, ongoing economic difficulties and increased pressure on IT departments to provide robust services create an incentive for colleges and universities to pursue cloud computing. Higher education has a special concern for intellectual property, and a cloud provider’s policy about ownership of IP might contradict institutional requirements. Cloud security is at least as much about policy as about technology. Whether in a private cloud with other institutions or contracting for commercial cloud services, colleges and universities must develop policies for how IT systems function in each institution’s context. These policies might also include security requirements for cases when individual faculty or departments obtain cloud services without oversight from a central IT authority.

EDUCAUSE

EDUCAUSE is a nonprofit membership association created to support those who lead, manage, and use information technology to benefit higher education. A comprehensive range of resources and activities is available to all EDUCAUSE members. The association’s strategic directions include focus in four areas: Teaching and Learning; Managing the Enterprise; E-Research and E-Scholarship; and the Evolving Role of IT and Leadership. For more information, visit educause.edu.