Addressing Cloud Data Ownership and Control Concerns

The global pharmaceutical company is a privately held multinational pharmaceutical company with multiple subsidiaries and entities. The company engages in research, development, production, and marketing of prescription and over-the-counter medicines and healthcare products. They are a midsized company with thousands of employees across the globe.

The company's IT procurement and deployment approach follows a decentralized model in which each entity subsidiary hosts its own servers and data centers. There are three functional organizational pillars maintained within its technology and IT services division: Technology Planning, Enterprise Architecture and Data Services, and Production Services. The division is staffed by dozens of IT engineers with managed services providing support for thousands of clients across dozens of sites; while managing an infrastructure of thousands of components. Their existing infrastructure includes hardware, software, services, and virtualization from multiple top vendors including Microsoft, VCE, Dell, Oracle, EMC and VMware.

Challenge

The company has adopted several cloud-based services for applications that do not process or store critical or regulated business information, such as Web conferencing, Spam filtering, compliance training and tracking, and travel and expense management. The global pharmaceutical would like to expand cloud computing usage to business critical applications, moving low value servers to cloud providers, as well as moving commodity applications to the cloud as appropriate.

Concerns about the loss of control and ownership of corporate data, however, stand in the way of realizing more efficiencies and operational benefits through broader adoption of cloud-based services. These concerns relate to:

- Compliance with regulations governing the security, privacy and confidentiality of healthcare data.
- Safeguards to limit exposure of its intellectual property when it is stored and processed in the cloud.
- Lack of visibility into service provider responses to information subpoenas that can result in a breach of confidentiality or loss of data.
- Compliance with international data residency requirements that preclude data leaving a jurisdiction in the clear.

Addressing HIPAA and HITECH

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) regulations explicitly specify the need to secure protected health information (PHI) and electronic protected health information (ePHI). The requirements apply to covered entities (CEs) and business associates (BAs) who store and exchange PHI. Additionally, unsecured electronic data at rest must be encrypted, according to both the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standard (FIPS). These standards are comprehensive and require BAs and CEs to significantly change the way electronic data is managed and transferred.

> "Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must: Implement a mechanism to encrypt and decrypt electronic protected health information."
>
> *HIPAA Technical Safeguards, Encryption and Decryption*

As described in the HIPAA Technical Safeguards, Encryption and Decryption (164.312(a)(2)(iv)) and Access Control (164.312(a)(1)) sections, encryption is recommended as a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text.

Addressing Ownership and Control of Cloud Data: Security, Residency and Unauthorized Disclosure

The global pharmaceutical invests considerable resources in the development of new drugs over an extended period of time with multiple parties: partners, clinical research organizations and regulators. While the cloud service provider can attest to the security of the environment based on a framework like the Cloud Security Alliance's Cloud Control Matrix, the global pharmaceutical company requires an independent mechanism to protect its intellectual property while resident in the cloud. Security concerns include attackers targeting the cloud environment, malicious actions of an administrator at the cloud provider, and potential intermingling of data in a compromised multi-tenant environment.

Similarly, a common challenge to cloud migration within the pharmaceutical/healthcare industry is confidentiality and sensitivity to a service provider's compliance with government subpoenas. Pharmaceutical and healthcare companies maintain sensitive information related to research, clinical study results, and personal medical history. It is critical that this sensitive information remain in the company's confidence, without any forfeiture of attorney-client privilege.

Data stored in the cloud resides within the cloud service provider's jurisdiction. If the company stores the sensitive data at a cloud provider and the service provider is faced with a subpoena or other request from the government, they must comply and disclose the global pharmaceutical company's data to the federal government body. The provider may notify the global pharmaceutical after the fact, or in cases of blind subpoenas, not at all.

> "The conversation comes up regularly...In all cases that Microsoft is subpoenaed to provide customer's data we will comply. This is a deal blocker to some customers."
>
> *Source: Microsoft Account Executive, July 2011*

The global pharmaceutical is unaware of the physical location of data stored in the cloud rendering it incapable of addressing complex laws that govern the data in any jurisdiction in which it resides. This issue is magnified for multinational companies which must comply with the EU Safe Harbor and US Patriot Act, restricting data residency.

The Vaultive Solution

Vaultive provides a data encryption solution that enables organizations to utilize cloud-based services while maintaining complete control over data security and the privacy of data. By providing the ability to encrypt

data before it leaves the trusted network and maintain persistent encryption of data while it resides in a third-party environment, Vaultive enables organizations to meet regulatory requirements for securing data at rest and protecting personally identifiable information (PII). Vaultive's proxy-based approach ensures that the protection is implemented transparently for end users; no changes to the application are required and the company's IT department retains ownership of the encryption keys. Vaultive does not interfere with standard email security features such as malware and anti-virus protection. No software or agent is installed on a client device or mobile phone, and tasks are completed without compromising functionality or performance.

The global pharmaceutical implemented Vaultive for Exchange on a selected subsidiary as part of an initial migration to Microsoft® Office 365. As part of the migration process, all email data is encrypted at the Vaultive proxy located at the global pharmaceutical company's site, securing the data before it travels to the Office 365 environment. The data remains encrypted throughout its lifecycle: while in-transit, at-rest, and in-use. The data is only decrypted once it reaches the intended recipient, having returned back through the Vaultive proxy at the edge of the global pharmaceutical's trusted network. The encryption keys, which are located within the Vaultive appliance, reside within the global pharmaceutical's trusted network, thereby allowing the global pharmaceutical to maintain full control of the data.

Vaultive encrypts the data using standard 256-bit AES encryption. Through proprietary extensions, the encryption enables the data to be indexed, searched, sorted, and otherwise processed without ever being decrypted in the cloud.

> "Companies such as Vaultive are creating technologies that enable these capabilities [storing sensitive information in the cloud] to become a reality."
>
> *Source: Global Pharmaceutical Executive*

With Vaultive, the pharmaceutical company implements the necessary controls to achieve compliance with the access control and encryption decryption requirements mandated by HIPAA and HITECH.

Because the data is encrypted at all times while outside the global pharmaceutical's trusted network, any authorized access or breach will only yield data that is an encrypted format. Similarly, in the case of data intermingling in a multi-tenant environment, only cipher text is exposed.

When Microsoft is served with a subpoena and law enforcement agencies or other government entities request access to the company's data residing on the cloud-based service, Microsoft can comply with the requirement but only discloses encrypted data that amounts to useless gibberish. Microsoft does not hold encryption keys nor do they have any access to them. To gain access to the decrypted data, the requesting government authority must contact the global pharmaceutical company directly, allowing them to maintain control of the data disclosure process via the standard client-attorney privilege process.

Since data is encrypted on premise at the global pharmaceutical site, prior to the transmission of the data to the Office 365 environment and the encryption keys are held within the same location, the company remains in compliance with local jurisdictional

requirements and regulations for data residency and data-at-rest protections. Once data is encrypted with keys that are maintained in the same jurisdiction, the encrypted data is no longer restricted to a specific geographical location.

Evaluation

The Vaultive deployment was successfully completed in tandem with migration to Office 365 with minimal disruption to normal business operations and zero loss of data or emails. The implementation was completed on time and within budget. Vaultive's encryption was implemented seamlessly with standard email security features such as malware and anti-virus protection. Employee feedback indicated that the implementation of Vaultive's encryption for all email data is entirely transparent to the end users. Additionally, employees and general users reported that the encryption does not compromise functionality, performance, or negatively impact the end-user experience.

Since no software or agent is installed on a client device or mobile phone, there is no additional need for IT management resources – reinforcing the value to the organization of moving to Office 365.

Future

Vaultive is a cloud data encryption platform which enables organizations to realize the cost savings, enhanced productivity, and operational efficiencies of the cloud while maintaining data security, control and compliance advantages of on premise computing. Data secured by Vaultive remains encrypted in-transit, at-rest and in-use within the cloud, while the organization maintains control of the encryption keys. Having successfully implemented the migration to Office 365 within one of its subsidiaries, the global pharmaceutical has developed a set of operational and technology best practices the company can re-iterate across all subsidiaries for a phased approach to cloud adoption.