The foundation history of magnolia electronics and its most famous innovations

Business, Company

Magnolia Electronics is an information technology company based out of the Southern United States and services the medical community. Magnolia Electronics provides hospitals and medical offices with software to monitor and store patient information, essentially following the established guidelines of traditional electronic patient record storage. Founded in 2015, Magnolia has grown quickly and services hospitals in 10 states with close to 50 clients. In recent months Magnolia has suffered several attacks to the Cloud storage functions which have affected the company's ability to utilize Cloud computing effectively. The Cloud computing infrastructure is designed to work on one of three types of architecture frameworks, SAAS, PAAS, or IAAS. Magnolia's software framework is designed to be a software as a service (SAAS), meaning that the company hosts the service and provides it to many users over the Internet (Munir & Palaniappan, 2013). Data security in Cloud computing is more complex than in traditional formats due to the disbursement of data across devices and networks. Each Cloud computing technology has its own unique risk factors as far as data security, but the concern is primarily when applications are run beyond the established firewall and move closer to the public domain.

For Cloud computing there are several inherent issues for data security, governance, and data management including privacy and trust issues. These issues are often made worse when employees use software on their own personal devices. If Cloud computing is to become a necessary and viable utility for Magnolia Electronics then aspects of data security must be addressed in the implementation plan including the following: safety mechanisms, data confidentiality, cloud server monitoring (or tracing), and

avoiding possible internal threats such as illegal insider operations and software hijacking. Some of the threats which are prevalent with Cloud computing are the issues of lost control over infrastructure when business models change (Cloud computing changes the way IT services are delivered) and the multi-tenancy nature of the shared technology—in addition to the obvious concerns of service hijacking, data loss and leakage without proper backups and disaster protection, identity theft, and malicious insiders. The following proposal will detail the primary uses and purposes of the software, the current literature on the subject of data security, the methodology of the proposal, the goals and objectives for the project, and the project deliverables in line with the need to secure Cloud data.

Magnolia Electronics has revolutionized the electronic medical records (EMR) landscape by developing a mobile device which can read patient information by scanning the code on hospital wristbands that contain the patient’s unique identification number for their records. The device operates with the hospital network and there is a seamless transition of data from the device to the stationary computers used in the facility to provide real-time information to the medical team. With the prevalence of electronic record keeping and mobile device usage there has been an increased focus on mobile data breaches as of late, mostly because it is easy to access any device connected to a network which has been hacked. Not only must the network be secured to protect data but all assets which are utilized for data collection must feature network security features as well.

This device reads the barcode-like identification on the patient’s wristband and immediately sends alerts and notifications to the nurse’s station when patients have been checked in and out of rooms or wards. These devices ultimately help to keep track of patient activity for the medical teams, but the software also must store patient information. If the devices themselves are breached, then all sensitive stored patient information is compromised. If the solution were to simply allow medical professionals to use their own device (BYOD, short for Bring Your Own Device) the responsibility would still be on the device developer to have proper network security functions installed. For example, this device has the capacity to install applications. This itself is a security concern which would require that part of the implementation of security procedures involve employee training on network and data security to avoid any unnecessary breaches as the result of unsecure downloads or application usage.

The devices themselves run on Windows software and the medical information software—otherwise known as electronic record monitoring (ERM)—is capable of being downloaded as an application from the company’s homepage via an access code and administrator account information which must be submitted. Each medical professional is provided an individual access code and account identifier along with a password to add a layer of security. However, BYOD policies are highly insecure compared to the company’s mobile device since an individual’s phone, computer, or tablet is not subject to the same security regulations that the company’s devices are.

Magnolia Electronics has identified the chief data security concerns that the company faces and has decided to implement the use of an End User Service Portal. The End User Service Portal will become a third-party certificate authority which will issue tokens for service to the users. Once users have joined the End User Service Portal they can utilize or purchase cloud services from the single service provider, which would be Magnolia Electronics. Not only would the users have logged interactions and uses of the software travel through the client's virtual private network (VPN), which is strongly recommended, they would also immediately be authorized and monitored by the certificate authority. Composed in the End User Service Portal would be access controls, security policies, service configuration, auditing management, key management, as well as the virtual environment which provides secure access control via the client's VPN and cloud service. Not only would this provide data security, but the recommended element of Single Sign-On (SSO) would increase productivity and make it easier to use the services.

The scope of the project includes acquiring the third-party certification software through purchases, designing and implementing the End User Service Portal, testing the portal for effective data security measures, making adjustments to the software to include SSO and unique password generation, and finalizing documentation of the Cloud computing architecture framework. This project's primary deliverable is a secure single access user experience by utilizing the End User Service Portal to secure

data and detect dual-activity from single users, thereby monitoring for incidents of hacking when the software is in use and when it is idle.