Why
Drones
Are The Next
Internet
One of the most frequently used methods for electronically storing maintenance data is a computerized maintenance management system (CMMS). CMMS systems hosted on the Internet (the Cloud) are becoming more and more common. But is your maintenance data safe when it is hosted on the Cloud and how does this compare to maintenance data stored on a local computer? In this article, some of the techniques used by cloud-based CMMS companies to ensure your data is secure are described and compared with the security of a local installation. While the security of local installations varies wildly, in most cases, the data on a cloud-based CMMS is more secure than on a locally hosted CMMS.

Where Is Your Data Stored and Is It Physically Safe?

Reputable cloud-based CMMS companies will store your data in an advanced and dedicated data center. The only business model of these data centers is to provide secure data storage and move this data safely to and from customers. These data centers are run by some of the biggest companies on the Internet, such as Google and Amazon. The expertise of these companies in storing their own data safely and securely led to the formation of new businesses that provide these services to other customers, including CMMS customers.

Data centers are typically nondescript buildings within major city centers. Inside, they have banks of computers. These computer banks are secured like a bank of money. All people, including data center staff, need to pass through multiple levels of security authentication to gain access to the computers and the supporting infrastructure.

Compare this physical security at the data center with a solution hosted on your own computer. A local installation is probably stored in an insecure room that is accessed by many people, including a cleaning crew. Alone. At night.

Data centers are incredibly secure in comparison.

Data Loss

Data loss can occur due to several reasons. Data can be physically stolen, deleted, or overwritten. None of these losses are realistic for a reputable, cloud-based CMMS run from a reputable data center.

First of all, the physical security measures in data centers essentially guarantee that theft of data storage devices from a good data center is impossible.

Second, data centers run multiple redundant backups of all data in several geographically distinct buildings. In effect, a backup hard drive containing the same information (but in a different building) would be ready to go almost instantly if data were to be lost for reasons including breakdown, theft, or environmental hazard.
in the CMMS Cloud
Addressing Concerns About Cloud-Based CMMS Solutions

In addition to the multiple redundant backups, a cloud CMMS solution will never permit the CMMS to be accidently uninstalled, nor will it need to be reinstalled when you upgrade your desktop computer.

With all these measures, you can be virtually assured that the data cannot be stolen, lost, or accidently overwritten with a reputable, cloud-based CMMS company.

Data Availability

Your data availability is the percentage of time your data is available, ready for access. This is a critical parameter because there is nothing worse than having a CMMS unavailable when it is needed.

For a cloud-based CMMS, part of the data availability calculation is the data center’s availability. Most data centers guarantee a minimum uptime percentage of 99.95 percent. Most perform much better than this.

Another component of cloud-based CMMS availability is the application availability. This is the amount of time the CMMS is available, excluding the small amounts of time when planned system upgrades are performed overnight. Reputable CMMS companies will record these outages and be happy to tell you their performance over the previous year. For example, in 2013, a leading provider of cloud-based CMMS solutions had a 99.991 percent availability over the entire year. Does your locally hosted CMMS achieve availability this high? Do you even measure it? When you do measure it, make sure it is a fair comparison by including all of the unplanned unavailability of the local system.

Furthermore, because a cloud-based CMMS is viewed over the Internet, it can be accessed at anytime from anywhere with an Internet connection. If you really want to, you can check your CMMS on your mobile phone while at the beach!

Web Security Against Hackers

Security against hackers is a critical element of any cloud hosted program. Data centers have systems in place to record and stop all classes of hacker attacks, including attacks based on denial of service (DoS), man-in-the-middle, IP spoofing, port scanning, and packet sniffing. Furthermore, exceptional CMMS companies will use irreversible hashing algorithms to protect sensitive data, like passwords, from being viewed in plain text by anyone. These measures combine to protect your data from thieves.

Data Sent Via the Web to the Data Center

Cloud-based CMMS providers also need to protect your data while it is being sent to and from the data center. Banks and other important Internet services, like e-mail, face a similar problem and they use a secure sockets layer (SSL) encryption technique to guard against it. Good CMMS companies use exactly the same technology with the same level of encryption. You will notice a padlock symbol in your browser when SSL is being used by your CMMS to stop hackers from observing the data being sent.

Access Control

The last security vulnerability that exists in both cloud and locally hosted CMMS systems is access control. On some locally hosted CMMS versions, anyone can use the computer on which the CMMS is installed and make changes to the CMMS. This is not permitted in a cloud-based CMMS. Users have to log in before they have any access to the CMMS. Then, because they are logged in, their actions are recorded. As a consequence, in the future, you will be able to determine who did what and when.

Conclusion

Cloud-based CMMS systems are incredibly secure. The data is stored in physically secured locations, with highly secured access controls. There is always a live backup of your data at another data center ready to take over in the case of a system failure in the primary data center. Furthermore, there are frequent historical backups of all data for protection in the unlikely event of a catastrophe. Hackers are thwarted using the latest techniques and your data is encrypted while being transmitted to the data center using the same methods adopted by the world’s largest financial institutions. In addition, because your users have to log in to their system, you will have a record of every change made in the system and by whom.

If you are still worried about using a cloud-based CMMS, you need to compare these security measures with a locally hosted system. Is your computer physically secured from other people? Do you have a live backup and regular historical backups? Do you have protection from hackers? And what about availability, can you guarantee a 99.95 percent uptime and access from anywhere with an Internet connection?

When you do a fair comparison, it is likely your own security measures will need improvements to match those provided by a reputable, cloud-based CMMS provider.