Why Data Management Review Is Vital For Enterprise Health

Contributor: Michael Lazar

Posted: 03/08/2016 12:00:00 AM EST

In case you missed it, the United States government (FBI) is attempting to force Apple, via the US legal system, to create a version of iOS which would allow it unlimited attempts to use "brute force" to guess and unlock the password of an iPhone.

Should Apple comply, it will enable the government to bypass an important security feature of iOS which, after ten incorrect password attempts, erases the data it contains.

While Apple and the FBI are arguing the case through the US legal system and in the court of public opinion, one fact from the case jumped out, and I believe it needs some discussion.

The phone in question was provided by an employer to an individual. At the US government's somewhat hasty request the employer was able to reset the employee's Apple ID password without issue and provide backups of the data to the government, as lawfully requested. Except there was a problem: *the phone itself had not completed a backup in approximately six weeks.*

There is some question as to whether the user disabled the cloud backup function or if the device had simply not been connected to a known network where the backup would be completed automatically.

This raises two questions that every enterprise administrator should be asking. One, how is it possible that the security profile would allow the employee to change the auto-backup setting? And two, why was it not obvious that backups had stopped working approximately six weeks prior to anyone looking for them?

Imagine if critical corporate resources (physical, virtual or cloud based) had not been backed up in six weeks? It would have been considered a catastrophic failure of policy. No one would have excused the situation.

In a seemingly unrelated event, a US hospital was the subject of a Ransomware attack. Somehow, malicious code was introduced into the environment and patient records were encrypted and held for ransom. Ultimately, the hospital was forced to pay.

What connects these two incidents? The answer is simple: poor data management. And both incidents clearly demonstrate that if robust data management policies aren't instituted, data is vulnerable to both attack and disappearance.

Most enterprises need to rethink their data management policies. They need to make sweeping changes and they need to implement them. Data today is no longer locked up in your datacenter or even in your employees' laptops and desktops (you remember desktops

right?).   Frequent access to critical data is extended all the way from your data centre and any cloud operations to desktops, laptops, tablets, mobile phones and now even wearable computing technology.

The following steps need to be set in place:

1. **Create a functional data map**
   Create a functional map of where your data resides and how it is accessed. This is not a one-time event; it needs to be reviewed and revised on a regular, diarized, basis.

2. **Label your data**
   Assign a risk-level classification to each piece of data. Label each with what would happen to your business if this data were lost, destroyed, tampered with or accessed without authorisation. This step can be the most involved and generally requires business stakeholders as well as technologists to complete.

3. **Review your data protection technologies and policies**
   Now that you have a map and labels, it is time to review how each piece of data is backed up and protected. Does the mechanism used to protect the data match the classifications?   What are the polices around data retention? How long is data kept? Does the technology used align with those policies?

4. **Develop a remediation plan and implement it**
   The above process may reveal gaps between what the enterprise considers critical data and how it is protected.

Unfortunately, data management is frequently an afterthought and when it is needed the most, it can be too late. Starting a data management review process will enable your enterprise to better understand how data is produced, consumed and protected. Ultimately undertaking this review will strengthen your enterprise when a "data event" occurs.

Original article – http://www.enterprisemobilityexchange.com/eme-big-data-analytics/articles/why-data-management-review-is-vital-for-enterprise