Protect your company data by encrypting mobile devices

Tuesday 15 March, 2016

With the rise in organisations adopting BYOD (Bring Your Own Device), it is no surprise that it is increasingly common for company data to be stored inside personal mobile devices. These devices, such as USB sticks, mobile phones and tablets, are important means to support more flexible business and working environments, and make it much easier for employees to work at home or whilst travelling.

However with constant technological innovation comes new risks, and technology designed to increase productivity and collaboration may cause or enable a data breach. Becoming more popular are impressive apps which can integrate with company systems to sync, transfer and store data in real time. This sounds excellent for businesses and their employees, but how good are these apps at keeping user data safe and secure?

While devices are shrinking in size and increasing in performance, they are also lost or stolen more easily - and when employees lose their devices, they are losing corporate data as well, putting companies at risk. What's to happen if a lost device falls into the wrong hands? Data stored inside could (and often does) be used to breach company systems, which can lead to serious consequences for the company should that data be highly sensitive.

Some mobile device statistics

- 93% of organisations have mobile devices connected to the corporate networks
- 67% allow personal devices to connect
- 67% cite securing corporate information as greatest BYOD challenge
- 53% report there is sensitive customer information on mobile devices
- 94% indicate lost or stolen customer information is grave concern in a mobile security incident

Source

How it can be managed

Rather than throw up barriers to adopting BYOD, and other technological trends with the potential to increase company productivity, IT departments should evolve their security strategies to ensure both company-issued and employee owned devices do not pose a data protection risk should they go missing.

Egosecure's Removable Device Encryption ensures that stored data cannot be accessed or used by unauthorized parties. Password-based encryption and decryption can be achieved on any Windows computer, with full transparency for authorized users. The encryption is file-based, and various encryption types are available (for the whole company, for individual users or for certain user groups). It is also possible to use multiple encryption types for one medium.

This provides organisations who allow employees to store information on mobile devices with greater protection from data breaches, subsequently giving IT departments a peace of mind!

For more information, visit http://egosecure.co.uk/

Media:

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Data Security :: Device Encryption :: Data Loss :: Data Protection :: IT Security :: Customer Data :: Egosecure :: Removable Device :: BYOD ::

Scan Me:

Company Contact:

Egosecure

T. 07912 097542
E. admin@egosecure.co.uk
W. https://egosecure.co.uk/

View Online

Additional Assets:
http://egosecure.co.uk/

Newsroom: Visit our Newsroom for all the latest stories:
https://www.egosecure.pressat.co.uk