The Downside to Dropbox

The 7 Risks Of Dropbox To Your Corporate Data

JR-TECH

Delivering Trouble-Free IT

Introduction

- With the proliferation of cyber crime, where information is power, Dropbox is similar to an open source for business information.
- Dropbox for many is what “cloud computing” represents.
- Business owners and employees of companies are currently using Dropbox for business applications in ways that it was not intended.
- Businesses are allowing employees to BYOD (Bring Your Own Device) for work. This reduces the security and control of business data. A more mobile workforce, places greater pressure for file sharing and access from multiple points.

- Background:
  - Dropbox is a leader in mobile file access with over 200 million users.
  - Dropbox is easy to install, easy to use and consumer friendly.
- Issue:
  - What works for sharing family vacation photos, does not apply to securing valuable business data.
  - The security, legal and business risks that are involved in using Dropbox for business involves unacceptable risk.

Risk - Data Theft

- Because Dropbox is so easy to install, employees are using it without the permission of the owner or the IT department. Employees can easily replicate entire file servers on Dropbox so they can access their files remotely.
- Without oversight, employees can install and access company information across multiple devices. Personal devices are easier for hackers to penetrate in airports, coffee shops, etc…
- Personal devices are more likely to be lost or stolen. This directly places business data at higher risk.

BUSINESS INSIDER Tech Finance Politics Strategy Life

TECH More: Dropbox

Nearly 7 Million Dropbox Passwords Have Been Hacked

STEVE KOVACH

OCT. 13, 2014, 11:58 PM 44,024 10

FACEBOOK LINKEDIN TWITTER GOOGLE+ PRINT EMAIL

Nearly 7 million Dropbox usernames and passwords have been hacked, apparently via third-party services that hackers were able to strip the login information from.

The Next Web was the first to notice the leak on

Flickr/Ian Lamont/Dropbox In 30 Minutes

Did You Know –

112 smartphones are lost or stolen every minute in the US. That is a potential of 57 million data security incidents per year!

JR-TECH

Data Loss

- Without the ability to monitor the movement of files or versions of files across user end points, Dropbox can improperly backup file revisions on employee devices especially if the endpoint is compromised or lost.
- The implication is, without IT oversight and visibility, there is a higher probability of losing a document or versions of files. There is no ability to restore the most current version of files, or the ability to regain a lost file or any version.

2 Questions For You –

How many of your employees have Dropbox on their personal smartphone, tablet or laptop?

How do you know if they do or not?

Silent Data Corruption

- In a study by CERN, the European Organization of Nuclear Research, observed that 1 out of every 1,500 files is corrupted silently.
- Stored data in the cloud is subject to the integrity of the storage provider. Most consumer file sync services do not implement data integrity assurance systems to guarantee end to end data integrity. SDC is common in large scale consumer storage systems.

Question For You –

Is your data guaranteed secure, or is your business data "silently" altered as bits are unintentionally changed?

Law Suits

- Dropbox gives any user the power to permanently delete and share files.
- The implication is, this can result in permanent loss of business documents. Additionally, it opens the business up to breaches in confidentiality and privacy agreements with third-parties and clients.

Ask Yourself –

How much liability am I responsible for that I don't know about?

Compliance Violations

- Many compliance policies require that files are held for a specific length of time, and can only be accessed by certain people.
- Dropbox has very loose file retention and file access controls.
- It is important for businesses that are subject to compliance regulations to employ strict control over the data they are entrusted with.

$201

This is the average estimated cost associated with each stolen record.

Imagine, if a company loses 1000 customer records that include 5 records each (credit card number, name, address, phone number), on average it will cost the company over a million dollars

Find out and do the math –
How many outdated file records are floating in "Shadow IT" programs like Dropbox that your company is responsible for? Multiply by $201!

JR-TECH

Loss of Accountability

- Without detailed reports and alerts across the system, there can be a loss of accountability.
- This means loss of tracking for changes to user accounts, organizations, passwords, and other entities.
- If there is no system in place to notify other admins of changes, and if a malicious admin gains access to the system, the configuration can be undone.

Are you a sitting duck? –

Are you setting your business up for failure by not being able to hold employees accountable?

Loss of File Access

- Dropbox doesn't track which users and computers touch a file at any given time.
- This can lead to problems if you are trying to determine the events leading up to the deletion, modification or creation of a file.

How much is your business data worth?

It is a choice between paying to give employees secure file sharing vs. a cheap option that can open your business to security breaches.

Conclusion

- Dropbox creates challenges for businesses concerning the control, visibility and security of their data.
- What typically happens is an employee sets up a personal Dropbox account and transfers business data, or replicates an entire server system to their account.
- Companies that blacklist Dropbox and formalize policies against using Dropbox find that employees will find a way around company firewalls to share files.
- The Solution:
  - Deploy a company-approved business application that will allow IT to control and provide safety of the data.
- Rationale:
  - This meets the desire of employees to securely access company data remotely across multiple devices.

For more information about cloud file sync capabilities for businesses, please contact JR-Tech at: 951-319-4080.