Reduce Your Risk

The Basics of Encryption and Compliance

CITRIX®
ShareFile

What is encryption?

It's a secret code that, when given a high enough level key, can't be broken. Encryption protocols translate your data into this secret code for storage and transfer. The right encryption tools use 128-bit or up to 256-bit encryption keys.

+ Currently, it would take a supercomputer one billion years to break a 128-bit encryption.

+ And 256-bit encryption? It would take 50 supercomputers checking a billion (1018) keys per second 3x1051 years to crack 256-bit encryption.

90% of companies are at risk for a serious data breach

$3.8 MILLION The average cost of a data breach.
23% increase since 2013.

Why do you need encryption?

1

You have a responsibility to your clients.

Your clients trust you with their personal information, so they expect a reasonable effort to prevent unauthorized disclosure or access.

2

You must comply with regulations and ethics codes.

Federal, state and industry guidelines regulate the exchange of sensitive electronic information for many businesses.

3

You should protect your reputation.

A data security breach will almost certainly result in the loss of clients, millions of dollars in fines and possibly generate negative publicity.

Source(s): https://otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented
http://www-03.ibm.com/security/data-breach/

Keep your sensitive data safe.

Professionals in regulated industries must take extra steps when storing or sharing electronic information that includes the confidential data of their clients. You need the right encryption tools to get the appropriate level of security for your business' data.

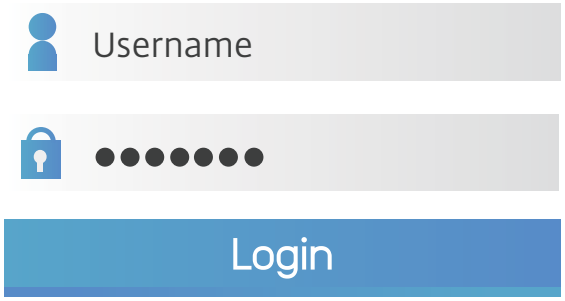
Why not rely on regular email?

Using an email service to exchange sensitive data is both unsecure and insufficient. Most email services have file-size restrictions for attachments, including 20 MB in Outlook and 25 MB in Gmail. Files bigger than that need to be broken up and sent in multiple pieces, putting your data further at risk.

Did you know...

Of the 1,390 major HIPAA breaches in 2015, 116 list email as the source of the breach.

Source(s): http://www.databreachtoday.com/email-breaches-lead-to-wall-shame-a-8695



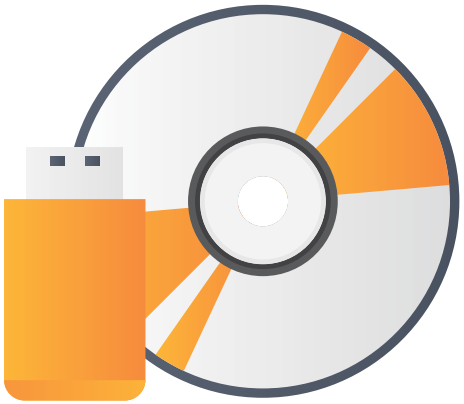
Why not rely on firewalls and passwords?

Your data is not protected by firewalls. Security breaches can occur when sharing and storing data on outside computers not configured correctly, including personal mobile devices. Passwords don't actually encrypt the data of your file - they just put that plain data behind a simple, short and easy-to-hack password.

Did you know...

One computer can test every possible combination of letters, numbers and special characters in a sixteen-letter password to crack it in as little as an hour.

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html



Why not rely on CDs, flash drives or fax?

Sharing and storing data by burning CDs or copying to flash drives is an easy way to lose or misplace critical data. There are size limits on them as well that may require multiple CDs or drives to store larger data.

Know the advantages of advanced encryption.

High-grade encryption can protect your data in transit (being moved, copied or transmitted) and at rest (stored in a location long or short term). The U.S. government uses the same encryption protocols to keep top secret information secure.

With the right file-sharing solution, you can have encrypted email, which protects the body and all attachments of an email from breaches if intercepted, and attach data securely up to 100 GB. Recipients can respond with an encrypted email as well.

Did you know...

One in three firms now use encryption for their data. By industry, financial services, healthcare, and pharmaceuticals are among the biggest users.

http://www.zdnet.com/article/encryption-more-and-more-companies-use-it-despite-nasty-tech-headaches/

What are your next steps?

Now that you understand the basics of encryption and compliance, decide how to implement them. Consider off-site storage services with cloud technology that offer you features like advanced encryption methods for file sharing and storage.

That way, you can focus on your clients while complying with federal, state and industry regulations anywhere, anytime.

REDUCE YOUR RISK AND RAISE YOUR GAME:

See why so many professionals trust ShareFile with their encrypted file sharing, storage and security needs.

Visit ShareFile.com to learn more.

CITRIX® ShareFile

Source links:
http://security.stackexchange.com/questions/43683/is-it-possible-to-brute-force-all-8-character-passwords-in-an-offline-attack
https://en.wikipedia.org/wiki/Brute-force_attack