
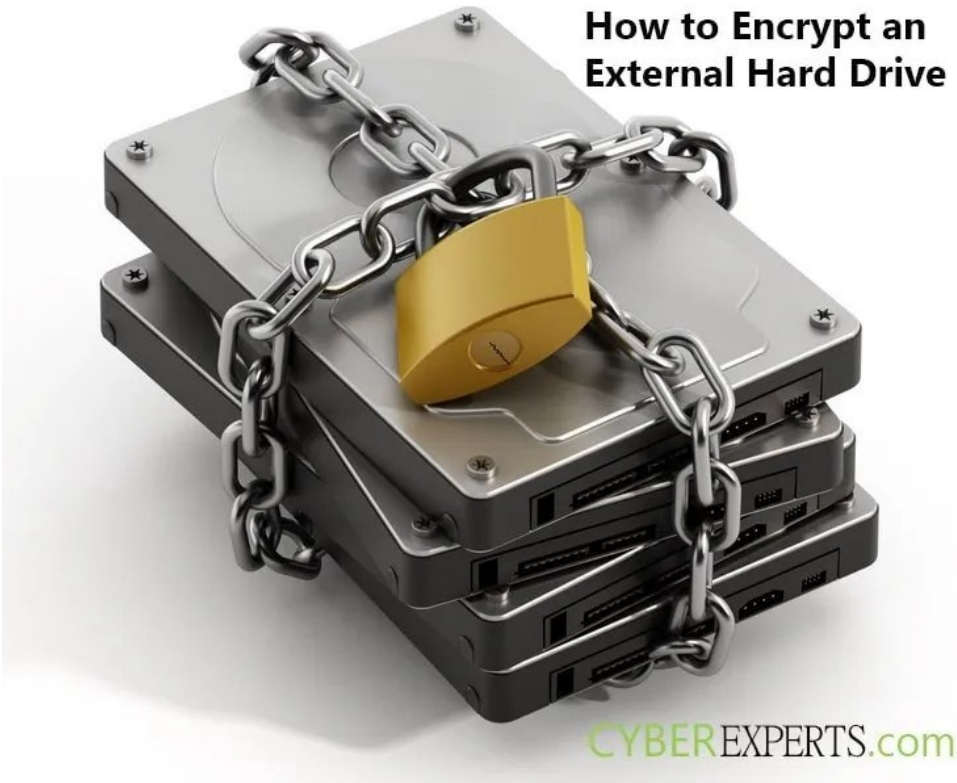


digitalforensics.com

 Digital Forensics Corporation

LEARN MORE



How to Encrypt an External Hard Drive

by George Mutune

digitalforensics.com

 Digital Forensics Corporation

LEARN MORE

The current average cost of a data breach increased by 10% to \$4.24 million. A data breach is an unwanted or unauthorized access to sensitive or personal information. As many businesses are concerned, data breaches are complicated hacks where hackers exploit system security flaws to access networks and

databases. As a result, they usually channel most resources towards securing the network perimeter by implementing **firewalls**, endpoint detection and response systems, **antimalware** products, and intelligent threat hunting capabilities.

All these and many others are vital to protecting customer and company data from increasing cyber threats. However, numerous organizations overlook securing one of the most used yet highly vulnerable information storage and backup methods – external hard drives. Protecting data stored in an external hard drive, including a USB flash drive and any other external storage device, is as essential as securing information stored in the cloud or a computer's internal hard drive. With more businesses becoming data-driven, the use of external hard drives has increased significantly. In 2020, **260.3 million hard disks were shipped globally**, compared to 316.3 million units in 2019. Despite lesser hard disks being shipped in 2020, hard drives remain critical to storing business data.

What is External Hard Drive Encryption?

An external drive or USB drive **encryption** is a fairly simple process. Essentially, it uses complex mathematical functions and algorithms to prevent unauthorized individuals from accessing the data stored in a hard drive. In addition, a hard drive encryption process provides an extra security layer since accessing the housed information requires users to provide a correct password or decryption key. The primary advantages of encrypting a hard drive include:

1. **Secure data transfer:** Companies use external hard drives to share data between internal departments or other interested parties. Malicious actors can intercept unencrypted data in transit for various illegal reasons, including selling to competitors or on the dark internet. In this regard, using appropriate hard disk encryption methods can enable secure information sharing.
2. **Adhering to compliance regulations:** Various regulations impose hefty fines for organizations that fail to encrypt specific information. Specifically, the Health Insurance Portability and Accountability Act (HIPAA) stipulates various **encryption requirements**, same as the **General Data Protection Regulation (GDPR)**. As such, encrypting external hard drives can enable organizations to comply with the mandatory compliance regulations.
3. **Enhanced data security:** Some of the rife challenges when storing sensitive data in external hard drives is that the data may be lost or stolen. Compromising the data stored in a lost hard drive requires a user to connect it to a computer and access it. Also, **insider threats** threaten

organizational information security and are often on the lookout for misplaced, unencrypted hard drives. Fortunately, applying the right hard disk encryption scheme ensures that stored data in a portable hard drive (removable drive) is inaccessible to malicious or unauthorized parties, even if the drive falls into the wrong hands:

4. **Preserving information integrity:** Unauthorized access to an unencrypted hard drive can lead to unauthorized data modification, deletion, or addition, thus compromising its integrity. Data integrity ensures that information retains its original state in terms of consistency, accuracy, and completeness. By using industry-standard techniques to encrypt a hard drive, an organization can prevent harmful actors from altering or modifying sensitive data, thus preserving its integrity.

Why you Should Never Leave a Hard Drive Unencrypted

1. A Healthcare Institution Fined Heavily Due to HIPAA Compliance Violations

As mentioned earlier, encrypting external hard drives goes a long way in complying with various regulations. However, Fresenius Medical Care North America, based in Massachusetts, was forced to pay a huge fine **amounting to \$3.5 million** for violating HIPAA compliance requirements. In the 2012 incident, malicious individuals compromised the electronic health information of several patients after they stole unencrypted hard drives and USB drives. Since HIPAA requires companies with access to health data to apply robust encryption standards, the health institution was forced to pay the fine for failing to do so. Such a huge penalty can cripple most businesses.

2. Unencrypted Hard Drive with Seven Years' Worth of Backup Data Stolen

Denton Health Group, a subsidiary of HealthTexas Provider Network, **lost an unencrypted external hard drive** that contained electronic health record data dating back seven years. The backup files contained numerous sensitive patient data types: phone numbers, insurance policies and provider details, clinical data, lab results, medication, medical practitioners' names, social security numbers, home addresses, and driver's license numbers. As such, the stolen hard drive affected both patients and medical staff. Such an incident should be a continuous reminder of why every organization must encrypt external hard drives using the recommended encryption methods.

3. Payroll Information of Facebook Employees Lost

A data breach that **affected 29,000 employees** occurred after someone stole

several unencrypted physical hard disks. At the time of the incident, the payroll employee had left the unencrypted external hard drives in the car only to find them gone upon returning. The stolen disks contained numerous sensitive information, including employee bonus and equity details, salaries, social security numbers, bank account numbers, and names. Attackers can use such information to execute more attacks, such as targeted **phishing** and identity theft attacks. If the payroll employee had encrypted the portable drives, they would have been useless to the thief since encryption prevents users without the correct key from accessing the data.

4. Health Data Compromised After Unencrypted Hard Drives were Lost

Centene Corp, a health insurance firm, reported that six unencrypted hard drives had been lost. According to the report, the stolen hard drives **housed protected health information of 950,000 individuals**, opening the insurer to hefty penalties while exposing the affected data owners to multiple risks. Although the company indicated that there was no evidence the information had been misused, the incident raises questions regarding the steps a company should take to protect data stored in external hard drives.

How You Can Encrypt an External Hard Drive

IT department heads require to sensitize employees to the essence of encrypting any removable media used to store data. There are four primary ways an organization can encrypt its external hard drives, memory cards, and USB flash drives. These are encrypting the whole drive, encrypting the files stored in the drive separately, utilizing hardware-encrypted drives, and applying third-party encryption services.

1. Encrypting Data Files Separately

Encrypting each file in an external hard drive is an effective way of keeping malicious users at bay. Essentially, the process involves protecting each data file with a password such that it is inaccessible without the correct decrypting password. In addition, a user can choose to store and encrypt data as a file system instead of individual files. Commonly used encryption methods include document processing software programs, such as Microsoft Word and Adobe.

File encryption is beneficial since it permits secure file sharing, whether through the internet or otherwise. For example, employees can share encrypted files via email without worrying that cyber attackers can intercept and use them. Even if hackers intercept them, they would still be useless since the attackers would still need a password or decryption keys to access the information therein.

2. Encrypting the Entire External Hard Drive

Technology has become an integral component of modern business operations, competition, and fostering growth. At the very least, every company has adopted some form of technology, including computer systems. Operating systems, such as Linux, macOS, and Windows, contain built-in tools that can enable anyone to encrypt an external hard disk drive used to store sensitive information. For example, the encryption tools in Linux, macOS, and Windows operating system are LUKS, FileVault, and BitLocker drive encryption, respectively. Some of the built-in external drive encryption tools allow users to create and store a recovery key in case someone forgets the password. Also, Windows users can back up

The built-in encryption tools are easy to use since a user must create a strong password to access the hard drive once it is fully encrypted. However, the primary restriction of using the tools to encrypt entire drives or USB sticks is incompatibility. For instance, encrypting an external hard drive using the BitLocker option encryption mode in a Windows computer means that it cannot be accessed in a computer running Linux OS, even if the user has the correct password. Windows OS users can store the recovery key in their Microsoft accounts.

Nevertheless, installing the relevant software program can enable access and use on any OS irrespective of the applied encryption method. The bottom line is full disk encryption prevents unauthorized access. One may opt to encrypt the files stored in the hard drive separately and still encrypt the entire hard drive to increase security.

3. Using a Third-Party Software

There are numerous third-party software programs an organization can use to encrypt its external storage drives. Most solutions apply industry-standard encryption schemes, such as Advanced Encryption Standard (AES), to provide the strongest encryption algorithms. In addition, some of the solutions are open source and free, which is critical to validating their validity and authenticity by evaluating the source code. Finally, although the encryption software may be platform- or OS-specific, they can be used to encrypt disks or each data file separately.

However, companies must use an encryption program from original vendors to

avoid using pirated or modified software that increases security risks to the hard drive data instead of protecting it. More frequently, using a modified encryption software can introduce security risks, such as backdoors or data exfiltration malware.

4. Utilizing a Hardware Encrypted Drive

Some portable hard drives come with built-in encryption capabilities. For example, a portable drive may contain hardware- or software-based encryption, where a user only requires to set a strong password to protect the stored data. Although they are highly efficient and easy to use when encrypting external hard drives, it is usually hard to determine whether they provide optimized data security or contain backdoors. However, the fact remains that encrypting an external hard disk is easy to secure important data.



George Mutune

I am a cyber security professional with a passion for delivering proactive strategies for day to day operational challenges. I am excited to be working with leading cyber security teams and professionals on projects that involve machine learning & AI solutions to solve the cyberspace menace and cut through inefficiency that plague today's business environments.

📁 [Cybersecurity, Encryption](#)

< [Connecticut Leads The Country With Cybersecurity Initiatives](#)

Sponsored Content

Musicians' Plane Crushes
Musicoholics

Toilet Paper Roll Under The
Toilet Seat At Night, Here's
xfreehub

Laugh At These Vacation
Pictures
Gloriousa

People On Medicare Are
Getting A Big Surprise This
Month
bestmedicareplans.com

[Pics] When The Cameras
Stopped Rolling, They Slept
In A Hotel
Fresh Edits

[Photos] She Suspiciously
Paid For Everything In Cash
For Years, Then Judge
The Primary Market

Recommended by | [▶](#)

Leave a Comment

Name *

Email *

Website

Post Comment



report this ad

Search



report this ad

Follow us to learn great things



Cybersecurity Encyclopedia

Advanced Persistent Threat

Adware
Antimalware
Banner Grabbing
Cloud Security
Cross-Site Scripting
Cyberattack
Cybersecurity
Defense in Depth
Denial of Service
Eavesdropping
Encryption
Espionage
Firewall
Insider Threat
Malware
Man-in-the-middle Attack
Network Security
Phishing
Ransomware



[report this ad](#)



© 2021 [CyberExperts](#)