Turn Key Solutions
225-751-4444 turnkeysol.com

THE IMPORTANCE OF FULL DISK ENCRYPTION

The first line of defense to protect data simply and effectively.

Data has become a critical asset for individuals and businesses alike. The proliferation of sensitive information, online transactions, and interconnected systems has made data more vulnerable to cyber threats. High-profile data breaches and cyberattacks have underscored the urgency of safeguarding data against theft, hacking, and other malicious activities.

What is Full Disk Encryption

Full-Disk Encryption (FDE) is a security technology that ensures that all the data stored on a computer's hard drive or storage device is automatically and transparently encrypted. This encryption renders the data unreadable without the proper decryption key or credentials. FDE protects data from unauthorized access, even if the physical storage device is lost, stolen, or compromised.

TurnKey Solutions

How Full-Disk Encryption Works:

- **Initialization**

  When FDE is set up, the user or system administrator defines an encryption passphrase or key. This key is used to encrypt and decrypt data.

- **Decryption Process**

  When data is accessed or read from the disk, it is automatically decrypted using the encryption key, rendering it readable for authorized users or applications.

- **Encryption Process**

  As data is written to the disk, the FDE software or hardware encrypts it using advanced encryption algorithms, such as AES (Advanced Encryption Standard). This process transforms the data into ciphertext, making it unreadable without the decryption key.

- **Protection at Rest**

  Even if the device is turned off or the storage medium is physically removed, the data remains encrypted, ensuring its confidentiality and security.

Turn Key

Turn Key Solutions

Real-World Case Studies

Data breaches that began with a stolen laptop:

- West Virginia-based Coplin Health Systems notified 43,000 patients of a data breach due to the theft of a laptop from an employee’s car.
- The Department of Health and Human Services has entered HIPAA settlements totaling nearly $2 million with two covered entities that reported relatively small breaches involving stolen unencrypted laptop computers.
- Recent breaches that originated on the endpoint include Eir, Raley's, and Health Plan, all of which involved stolen unencrypted laptops.

TurnKey Solutions

Cyber Security Statitics

53 seconds	A laptop is stolen every 53 seconds in the United States.
2 Million	Over 2 million laptops are stolen every year in the US
57 %	Laptop theft accounts for 57% of all identity theft
70 Million	70 mil smartphones are lost every year & only 7% are recovered
97 %	Over 97% of stolen or lost laptops are never recovered
1 in 10	1 in 10 laptop theft victims experience identity theft
3.5 Billion	3.5 billion is the total cost of stolen corporate laptops yearly
$49 K	The cost of a lost laptop for a business is an average of $49,246

TurnKey Solutions

Role of FDE in Mitigating Risks for Cyber Insurance

Cyber insurance has emerged as a crucial tool for businesses to mitigate financial losses resulting from data breaches and cyber incidents. Full Disk Encryption plays a central role in mitigating these risks by:

- Reducing the likelihood of data breaches: FDE prevents unauthorized access to data, making it significantly harder for cybercriminals to steal sensitive information.
- Lowering insurance premiums: Insurance providers often offer reduced premiums to organizations that implement strong security measures like FDE, as it demonstrates a commitment to data protection.
- Mitigating the impact of breaches: In the event of a breach, FDE can limit the exposure of sensitive data, minimizing the financial and reputational damage that can result from such incidents. This can lead to more favorable insurance outcomes.

TurnKey Solutions

Relationship Between FDE and Cyber Insurance

Full Disk Encryption (FDE) and cyber insurance are closely related in the context of data security and risk management. Cyber insurance is a policy that organizations purchase to protect themselves financially in the event of a data breach, cyberattack, or other cybersecurity incidents. FDE plays a significant role in this relationship:

FDE as a Risk Mitigation Tool

- FDE serves as a proactive security measure that helps organizations prevent and mitigate data breaches. By encrypting data at rest on their devices, organizations significantly reduce the risk of unauthorized access in the event of a physical theft or breach.
- Cyber insurance providers recognize FDE as a strong risk reduction measure, and they often encourage or require their policyholders to implement it as part of their cybersecurity strategy.

Compliance with Insurance Requirements

- Some cyber insurance policies include specific requirements or recommendations for security practices, including the use of encryption technologies like FDE. Compliance with these requirements can be a condition for obtaining or maintaining coverage.
- Organizations that can demonstrate compliance with such security practices, including FDE, may find it easier to secure cyber insurance coverage at reasonable rates.

Impact on Insurance Premiums

- FDE can lead to reduced insurance premiums for policyholders. Insurance companies assess the level of risk an organization faces when determining premiums. By implementing robust security measures like FDE, organizations demonstrate their commitment to data protection and risk reduction, which can result in lower premium costs.
- Cyber insurance providers may offer discounts or more favorable terms to organizations that have deployed FDE because it reduces the likelihood and potential severity of data breaches.

FDE in the Claims Process

- In the unfortunate event of a data breach, having FDE in place can impact the claims process positively. If a breach occurs but the stolen or compromised data is encrypted, it may not be considered a "data breach" in the eyes of the insurer, potentially affecting the coverage and financial liability.

Vulnerability of Unencrypted Data on Devices

Data Tampering

Unencrypted data can be altered or modified by unauthorized parties, compromising its integrity and reliability.

Data Theft

Anyone with physical or remote access to the device can easily access and steal sensitive information, leading to identity theft, fraud, or corporate espionage.

Regulatory Non-Compliance

Many data protection regulations and privacy laws require the encryption of sensitive data. Failing to encrypt can result in legal and financial consequences.

Turn Key
TurnKeySolutions

Potential Consequences of Data Breaches and Unauthorized Access

Data breaches and unauthorized access can lead to severe consequences for individuals and organizations, including:

Financial Loss

Data breaches often result in significant financial damages, including costs for breach remediation, legal fees, and regulatory fines.

Reputation Damage

Publicized data breaches can harm an organization's reputation, eroding trust among customers, partners, and stakeholders.

Loss of Intellectual Property

Unauthorized access can lead to the theft of proprietary information, trade secrets, or valuable research.

Legal & Regulatory Consequences

Non-compliance with data protection laws can result in hefty fines and legal actions.

Identity Theft

Individuals can suffer from identity theft, fraud, and personal information exposure, leading to financial and emotional distress.

TurnKey Solutions

Contact Us

Full Disk Encryption is not only a valuable security measure for protecting sensitive data but also a way for organizations to reduce their cyber insurance premiums and demonstrate their commitment to data security to insurers. It serves as a proactive security measure that aligns with the risk management goals of both organizations and insurers in the ever-evolving landscape of cybersecurity threats.

Our team of experts can help your business stay protected with our Endpoint Security and Data Encryption Services.

225-751-4444

www.turnkeysol.com

ask@turnkeysol.com

Baton Rouge - New Orleans - Dallas

www.turnkeysol.com/bookaconsult/

Henry Overton

President, Turn Key Solutions