Save the data—Self-Encrypting Drives

In 2015, a Texas Department of Transportation employee leaked data from an agency system used by Texas drivers to renew licenses and view vehicle registration records. The stolen data included the Social Security numbers of 2.7 million people who had driving or vehicle records. This ranks as the largest data breach in Texas history. In 2014, 1.4 million customer records were stolen from Humana. In 2013, the loss of an unencrypted drive containing personal records from UCLA Health made headlines. The theft was apparently handled by junior employees and involved protected discs.

4,817 Data Breaches

In total, 4,817 data breaches have been reported since 2005 with 898,584,384 records breached. These breaches, which often lead to the release of such incidents, which often lead to:

- **Sheer magnitude of breaches**
- **Inadequate protection**
- **Lack of standards**
- **Consistent breach notification**
- **Organization is more vulnerable than ever**

Self-Encrypting Drives

Sheer magnitude of breaches... Protecting the data

Data is more vulnerable than ever. The Chronology of Data Breaches shows that the average cost of a data breach is $3.8M.

The Internet of Things...

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

Hardware security benefits

SED Benefits

Compared to software-based encryption, Self-Encrypting Drives (SEDs) offer many benefits:

- **Encryption solutions, SEDs contribute to the TCG with a standardized approach and are widely adopted in most solid state and enterprise drives as well as HDDs and many USB drives.**

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

Protecting the data

- **Self-Encrypting Drives**
- **Save the data**
- **Zero impact**
- **Sanitize or re-purpose drives**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%

Dr. Robert Thibadeau, contributor to SED standards, predicts a rapid acceleration of SED adoption. "Any government department or other organization deploying SEDs can forget about hitting the headlines for the loss of an unencrypted drive containing personal records."

With SEDs, users benefit from:

- **Hardware encryption**
- **Ease of management**
- **Performance**
- **Simplicity**
- **Cost savings**

These drives are installed in:

- **Desktop systems**
- **Laptop and notebook systems**
- **Servers**
- **Workstations**

SEDs are easy to set up and manage remotely. They are highly effective and are self-encrypting by on-drive random encryption key generation in the factory. The encryption key is managed and software vendors exploit the encryption key.

Performance

According to the Ponemon Institute survey claims that 40% of CIOs believe that encryption is a primary defense against data breaches. Organizations that adopt encryption save on average $154 per record compromised.

Re-encryption

Encryption Key:

10%