Save the data

Self-Encrypting Drives

In 2013, International Data Corporation (IDC) estimated the growth of global data volume over a six year span at ten-fold, from 4.4 zettabytes to 44 zettabytes. Much of it relates to the advent of the Internet of Things (IoT), connecting a vast universe spanning from jet engines and cars to mobile phones and, yes, dog collars.

The Internet of Things is...

- fed by sensors soon to number **in the trillions**
- working with intelligent systems **in the billions**
- involving **millions of applications**

10%

Data just from the embedded systems - the sensors and monitoring systems - already accounts for 2%, and by year 2020 that will rise to 10% of the digital universe

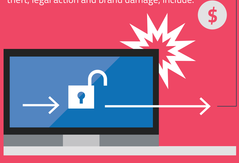
Sheer magnitude of breaches

Data is more vulnerable than ever, however. The Chronology of Data Breaches, which tracks compromises of personal information, reports:

4,817

Data Breaches

made public since 2005 with 898,584,384 RECORDS BREACHED in total. Examples of such incidents, which often lead to identity theft, legal action and brand damage, include:



1. **Nationwide Building Society** Missing notebook containing data of 11 million customers
2. **Humana** Company laptop stolen, along with a file containing customer information
3. **University of California** Laptop computer theft with graduate student application information including Social Security numbers
4. **UCLA Health** Valuable data on password -protected discs was apparently being handled by junior employees

The consequences can be devastating to businesses and individuals. Ponemon Institute reported in 2015:

$3.8M **Average total cost of data breach**

$154 **Average cost per lost/stolen record**

22% **Likelihood of a business being breached in the coming 24 months**

Protecting the data

Whether negligence or malice, data vulnerability cannot be ignored. One highly effective solution: self-encrypting drives (SEDs), which encrypt data automatically and transparently to users. Encryption is located in the drive controller (electronics) and is always on, providing a solution superior to less secure and performance-heavy software-based encryption.

With SEDs, users benefit from:

- Zero impact on hardware performance
- Seamless integration
- Remote SED management
- Constant encryption

Sanitizing drives

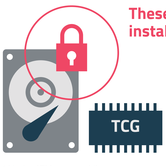
To sanitize or re-purpose drives, users or admins simply delete the encryption key and data is rendered unreadable, eliminating the need for time-consuming drive data-overwriting processes and breach notifications (state, federal, and international legislation often explicitly grant "encryption safe harbor" for encrypted data).

40%

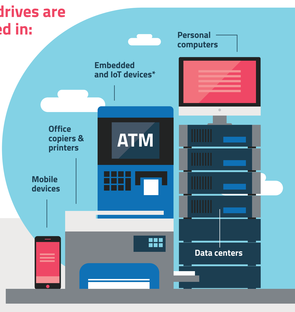
Ponemon Institute survey claims 40% of CIOs believe their employees routinely turned off their laptops' software-based security protection

Hardware security benefits

As an alternative to software encryption, hardware encryption based on TCG specifications is widely adopted in most solid state and enterprise drives as well as HDDs and many USB drives.



These drives are installed in:



* kiosks, ATMs, automobiles, industrial systems

SED Benefits

Compared to software-based encryption solutions, SEDs offer many benefits:

Transparency
No system or application modifications required; encryption key generated in the factory by on-drive random number process; drive is always encrypting

Ease of management
No encryption key to manage; software vendors exploit standardized interface to manage SEDs, including remote management, pre-boot authentication, and password recovery

Disposal cost
With an SED, erase on-board encryption key immediately for fast disposal and/or re-use

Re-encryption
No need to ever re-encrypt the data

Performance
No degradation in system performance

Standardization
Industry has widely adopted and contributed to the TCG and SED specifications

Simplification
No interference with upstream processes; easy to set up and manage remotely

$12

According to 2015 Cost of Data Breach Study from the Ponemon Institute, organizations enforcing the extensive use of encryption saved $12 per record

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".

www.trustedcomputinggroup.org

SOURCES: simson.net, ComputerWeekly, Privacy Rights Clearinghouse, Ponemon Institute, IBM, EMC

TRUSTED COMPUTING GROUP®