

*Stonewood, the creators of FlagStone present...*

## Software or Hardware Encryption – Are you Safe?

*Data Encryption* – no longer words that fly over your head, but rather fly around the press for all the wrong reasons. Marks and Spencer’s, Nationwide Building Society, HM Revenue and Customs, Driving Standards Agency and Ministry of Defence are just some of the companies and government departments that have fallen on the way side of significant data loss. Public confidence in those who hold their personal details is extremely low as a result of

<b>Nationwide Building Society</b>	Laptop stolen with 11m customer records, fined £1 million
<b>Marks and Spencer’s</b>	26,000 employee personal details
<b>London Metropolitan Police</b>	3 laptops stolen containing payroll details of 15,000 police officers
<b>HM Revenue and Customs</b>	25 million benefit records lost
<b>Driving Standards Agency</b>	3 million learner drivers details lost
<b>Ministry of Defence</b>	Laptop stolen with details of 600,000 personnel looking to join Armed Forces

these security breaches.

Companies and government departments alike are now realising the error of their ways and addressing their data security needs. A laptop is stolen every 53 seconds, 2 million are lost or stolen very year and 2,900 laptops were

left in London Taxis in just 6 months, so it should be of no surprise that Hard Drive Encryption is high on the agenda and for many organisations it comes down to a choice of either a software or hardware solution. Software encryption is the ‘quick fix’ for many, due to its lower initial outlay but sadly this is where the benefits of a software solution end.

### Software Encryption

Let us first review the key features and issues of software encryption as a data storage solution.

**STONEWOOD**  
Sandford Lane  
Wareham  
Dorset BH20 4DY  
United Kingdom

Tel: +44 1929 55 44 00  
Fax: +44 1929 55 25 25  
Email: [info@eclipt.com](mailto:info@eclipt.com)

Software solutions provide encryption from an application run from the computer and managed by an Operating System (OS) such as Windows for example. Its operation and success is directly dependent on the OS which means there will inevitably be performance degradation to some level. Some solutions come with the option of an opt-out altogether, but this makes it as vulnerable as it is flexible.

With the nature of software in mind, these solutions are also vulnerable to multiple attacks from trojans, viruses, malware and rootkits. Keys are kept on the hard drive which means they are open to discovery.

Implementation of software solutions can be time consuming and complicated. They all work with a specific OS release meaning that some may work with Windows Vista, but not Windows 2000 for example, and any organisations that haven't simultaneously upgraded all systems will be left with a solution that does not fit all.

Maintenance of software usually involves annual licensing and OS updates which are again time-consuming and costly. The larger the organisation, the larger an annual project becomes.

## **Hardware Encryption**

Now let us review the key features and issues of hardware encryption as a data storage solution.

Hardware encryption provides encryption of a laptop or desktop hard drive, external hard drive or external memory device and runs completely independent



from all Operating Systems (OS). It is not dependent on specific patches or service pack updates in order to execute.

There is no configuration, no ability to turn it off, no ability to disable it, it is completely transparent to the user and as such there is no performance degradation to the user or OS.

All methods of attack are ineffective. Data is immediately encrypted at all times and is safe from all attacks. Keys do not reside on the hard drive, making them impossible to read.

Typically, hardware solutions are government-accredited or recommended to store up to Top Secret level information, which only goes to prove its reliability and high level of security.

Finally, there is no maintenance work required and no maintenance costs involved at all. There is no annual license, no annual re-keying necessary and no OS updates to consider as the hardware works independent of the OS.

### **The Analysis**

There would appear to be advantages for each solution, so in order to make it easier to compare, we have compiled the following list of direct comparisons between the two solutions:

(Note. We have used our own FlagStone Hard Drive for the basis of this comparison between the two solutions)

<i>Area</i>	<i>Software</i>	<i>Hardware (FlagStone Hard Drive)</i>
<b>Operating System (OS) Independence</b>	Subject to OS upgrades and service packs. Not all releases from Microsoft and/or Unix/Linux are covered.	Operating system independent: <ul style="list-style-type: none"> <li>• All version of Microsoft Windows</li> <li>• All versions of Unix/Linux</li> </ul>
<b>Encryption Coverage</b>	Partial (e.g. My Documents) or Entire Drive often with opt-out facilities.	Entire Drive with 100% security 100% of the time.
<b>CPU Performance</b>	5-10% of CPU performance.	No performance degradation.
<b>Tamper Resistance</b>	Susceptible to side attacks including rootkits and trojans. Vulnerability at reboot and hibernation mode.	All methods of attack are ineffective, including discovery attack, brute force attack, steal twice attack and rootkits.
<b>Maintenance</b>	Annual Service Contracts. Operating System Updates. Annual maintenance and support costs.	24 month warranty with extensions available. No maintenance work. No maintenance costs. Free Customer Support.

When compared side-by-side, it is clear to see that there is a distinct advantage for hardware level encryption. It must be noted that there is a higher initial outlay in the cost of a hardware solution but in terms of a total cost of ownership over a period of

3-5 years, it is a sound investment without any re-occurring charges as is with software. For demonstrative purposes, we have identified the cost implications for a software solution against that of a FlagStone Encrypted Hard Drive below:

## FlagStone Hard Drive

### Cost of FlagStone

- Less refund on hard drive
- + Cost of one off key ( £10)

---

**Total cost of ownership**  
**Over 5 years**

## Software

### Cost of Initial Licence

- + Annual Licence Charge
- + Cost of annual Key ( £10 per annum)
- + Cost of annual transport to re-keying location
- + Cost of re-keying infrastructure
  - Personnel
  - Administration
  - Facilities
- + Cost of reapplying encryption after service pack updates

---

**Total cost of ownership**  
**Over 5 years**

## FlagStone

Our accredited range of FlagStone Hard Drives and our new Next-Gen range of FlagStone Ecllypt Hard Drives will protect all levels of data, from company confidential all the way up to Top Secret government data. Our hardware solutions are available as a direct replacement for your current hard drive, as well as an additional external drive. FlagStone hardware works independent of all operating systems, making it compatible with all versions of Windows and Unix/Linux, and all major laptop models. Our 'Fit and Forget' solution means that once installed, your data will be fully protected by a fully-transparent hardware that requires no further



maintenance or running costs. All drives come with an extendable 24-month warranty and free 24-hour customer support.

Furthermore if your laptop did unfortunately get stolen, you can be secure in the knowledge that your data is fully protected due to our drives' tamper proof design. Our latest Eclipt Hard Drives come with a number of additional features including increased drive capacity, support of up to 128 user accounts at any one time with 3 levels of user profile for flexible authority all within one simple-to-use Windows-based User Account Management software, and remote management capabilities.

For further information on any of our hardware solutions, visit our website [www.Eclipt.com](http://www.Eclipt.com) or alternatively contact us by phone or stop by our stand at InfoSec as detailed below.

### **InfoSec Europe 2008**

Come to our stand (K911) at InfoSec Europe, held at Olympia, London from April 22<sup>nd</sup>-24<sup>th</sup> 2008. Hear and see more about our Next-Gen Eclipt range of Encrypted Hard Drives for the corporate market. Tickets are free and can be registered for at [www.infosec.co.uk/stonewoodinvitation](http://www.infosec.co.uk/stonewoodinvitation). Here you can speak to our dedicated Business Development Managers, who will cater to your organisation's specific requirements for data protection and provide you with the ideal solution.

### **Free Demonstration**

If at any time you would like a free demonstration of our products or an evaluation unit to test, contact us on 01929 554400 and we would be delighted to arrange that for you.

*Software or Hardware Encryption – Are you Safe?*