

A Guide To Laptop Encryption



1 Table Of Contents

1	Table of contents.....	2
2	Introduction.....	3
3	Personal Data.....	3
	3.1 What Is Personal Data?	3
4	What Do I Need To Do?	4
	4.1 Assessing Where Personal Data May Be At Risk	4
	4.2 Ensure You're Protected	4
	4.3 Assessing The Level Of Risk.....	5
5	Solutions	6
	5.1 I Need A Solution. What Next?	6
	5.2 CAPS.....	6
	5.3 FIPS 140	6
	5.4 CCT Mark.....	6
	5.5 Accredited Solutions.....	6
6	Design Considerations	6
	6.1 Hypervisor Selection.....	6
	6.2 Hardware Consolidation	6
	6.3 Logical Topology.....	7
	6.4 VM Spread	7
	6.5 VM Migration.....	7
7	Approaches to Securing the Virtual Data Centre	7

2 Introduction

The trend towards an increasingly mobile workforce has created a new set of IT security challenges. Issuing laptops, PDAs, BlackBerrys and smartphones to employees is an efficient way for staff on the move to access the information they need. This is great news for any organisation provided that the data is held and transported securely.

A string of headlines in recent months suggests that security is being overlooked in the rush to arm remote workers with the latest mobile devices. Several high-profile cases of government laptops containing sensitive information being lost or stolen has led to the announcement that public sector organisations must encrypt all laptops that store personal data*. Private sector companies are also under pressure to protect the personal data that they hold. The Information Commissioner's Office (ICO) ordered Marks & Spencer to fully encrypt all its laptop hard drives in 2008, following the theft of one of their contractor's unencrypted laptops holding the personal information of 26,000 of its employees.

3 Personal Data

The guidance around laptop encryption is complex and this can be made even more so owing to confusion over what exactly personal data is.

3.1 What Is Personal Data?

In the wake of the HMRC data handling incident, the Government has clarified the definition of personal data as that whose release or loss could cause harm or distress to individuals. As a minimum, it defines this as any information that links an identifiable living person with information about them whose release would put them at significant risk of harm or distress. This could be information that could be used along with publicly accessible information to identify a person e.g. name, address (home, business or both), postcode, email address, telephone number, driving licence number and/or date of birth. Information whose release is likely to cause harm or distress includes sensitive personal data as defined by the Data Protection Act i.e. information relating to:

- racial or ethnic origin
- sexuality
- membership of a trade union
- political opinions, religious beliefs or other beliefs of a similar nature
- physical or mental health details
- commission or alleged commission of any offence
- proceedings for any offences alleged or committed

Further information on determining what is personal data can be found at:

http://www.ico.gov.uk/upload/documents/determining_what_is_personal_data/whatispersonaldata2.htm

<http://www.silicon.com/publicsector/0,3800010403,39169759,00.htm>

4 What Do I Need To Do?

The first step is to determine whether or not your organisation holds personal data. If it does then you need to decide if any changes are necessary to the way it's handled, stored and/or exchanged.

4.1 Assessing Where Personal Data May Be At Risk

A good starting point is for an organisation to review its level of risk based on the type of information stored and how it's handled. Perhaps the personal data held by your organisation is not stored on laptops or any mobile device but if it is it should be protected either by technical solutions such as cryptography or by considering procedural changes. For instance, it might be the case that the personal data has no real need to be held on laptops or indeed that a particular user doesn't really require the use of a laptop at all. At this stage, it's also worth considering how personal data is exchanged. For example, if it is sent out in the post on a CD then a whole other solution might be required.

It's arguable that in today's climate an assessment of risk doesn't have to be overly technical. As indicated by recent events, if an organisation loses a laptop containing personal customer records the chances are that the media will jump on it. Therefore, the risk that a party is mitigating against is often the potential damage to its reputation and loss of customers as a result of the media attention rather than damage due to the exploitation or exposure of the personal data the laptop contained. For some organisations, encryption is implemented purely for peace of mind. It means that the organisation can respond to the media by explaining that the lost data was encrypted and therefore could not be used illicitly.

4.2 Ensure You're Protected

View the Enforcement Notice served by the ICO to Marks & Spencer PLC at: http://www.ico.gov.uk/upload/documents/library/data_protection/notices/m_and_s_sanitiseden.pdf for a full description of what M&S were found to be in breach of.

It indicates that as a Data Controller, an organisation has a duty to comply with the Data Protection Principles and in particular the seventh principle which requires the organisation to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data, accidental loss or destruction of or damage to personal data.

Also, Paragraph 9 of Part II of Schedule 1 of the Act provides that: "Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

- the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle
- the nature of the data to be protected

4.3 Assessing The Level Of Risk

It may be useful to consider the e-Government Security Framework's impact level definitions when determining the potential impacts of personal data loss or exposure, and the security measures necessary to protect personal data held on mobile devices. The e-Government Security Framework defines four levels of confidentiality, which represent degrees of impact of disclosure of private information. Level 0 confidentiality is appropriate for transactions that do not include private information. Level 1 applies where the information exchanged is client specific but the impact of its exposure to the public would be minor. Level 2 confidentiality is suitable for transactions involving private information that could be considered sensitive and the disclosure of which could result in significant inconvenience or significant financial loss to any party, significant damage to any party's standing or reputation, significant distress to any party or assistance to or hindrance in detecting a serious crime. Level 3 confidentiality should be applied to private information regarded as very sensitive, the disclosure of which might result in substantial inconvenience, risk to any party's personal safety, substantial financial loss, substantial damage to any party's standing or reputation, substantial distress or assistance in the commission or hindrance in the detection of serious crime.

5 Solutions

5.1 I Need A Solution. What Next?

Once you determine that a technical solution is necessary to safeguard personal information held on mobile devices and equipment, the next step is to choose a solution that provides the appropriate level of protection. Many options are available, including solutions providing media or file encryption, whole disk encryption, secure remote access and strong authentication. A number of schemes exist to provide the consumer with assurance as to the effectiveness and validity of the vendors security claims. These schemes are discussed below.

5.2 CAPS

CAPS is a CESG-assisted products service that helps private sector companies to develop cryptographic products for HMG and other appropriate organisations. It is a government-approved scheme for the encryption of nationally protectively marked information (RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET). This is a top of the range scheme and contains products assured to protect information at Impact Level 3 and above.

5.3 FIPS 140

The Federal Information Processing Standard (FIPS) 140 is a US Government computer security standard used to accredit cryptographic solutions – including hardware and software. This accreditation is popular among public and private sector bodies that don't hold restricted information but that do hold private and sensitive data. FIPS 140-2 is appropriate to protect information at Impact Level 2 and below.

5.4 CCT Mark

The CSIA Claims Tested (CCT) Mark provides a government-approved accreditation for the public and private sectors. The CCT Mark is awarded following accredited independent testing to test that the security functionality of the product does exactly what its vendors claim. The CCT Mark is not exclusively for encryption products; it can be awarded to products that provide secure authentication, secure erasure and disposal, connection and network protection. The CCT Mark is assured to safeguard information at Impact Levels 1 and 2.

5.5 Accredited Solutions

For most organisations, that do not handle nationally protectively marked information, the level of accreditation offered by FIPS 140-2 or the CCT Mark is sufficient. Examples of mobile device encryption solutions that assure this level of cryptographic security include Check Point Pointsec full disk encryption and McAfee (SafeBoot) endpoint encryption. BitLocker Drive Encryption, which is included with Microsoft's Windows Vista and Windows Servers 2008 operating systems, is also approved for Impact Levels 1 and 2 and, if implemented according to the guidelines from CESG, it is approved for protecting Impact Level 3 national protectively marked RESTRICTED information.

6 Design Considerations

When designing a new data centre using virtualised infrastructure, or when planning a migration for an existing physical infrastructure, it is important to remember that virtualising an environment provides new challenges, compared with traditional designs.

6.1 Hypervisor Selection

The first thing to consider when designing a virtualised environment is which hypervisor you intend to use. Mainstream options range from the Enterprise class offerings from VMWare to the emerging Hyper-V from Microsoft, and the open source Xen and VirtualBox.

As the market leader and the first major virtualisation provider, VMWare's hypervisors have good support from third party enhancements, such as hypervisor firewalls and network virtualisation layers. VMWare requires a significant investment in terms of licence costs and software products, but remains the most broadly supported hypervisor. A number of VMWare's lighter products are available for free, such as VMWare Server, which can be used for proof of concept, development, and small-scale production environments.

Hyper-V is an emerging product which Microsoft is pushing as an alternative to VMWare and which is heavily integrated with Windows Server 2008. Hyper-V is attractive to existing Microsoft customers with a high level of previous investment in Microsoft products, and is being aggressively marketed at this demographic. At present, however, Hyper-V is poorly supported by third-party add-ons compared to VMWare.

Both Xen and VirtualBox are free open source hypervisors and differ significantly from the offerings from VMWare and Microsoft. At present, OS support within VirtualBox is relatively poor and many OS installations require add-ons. Xen is a more mature product which has some interesting management tools available. Depending on the base OS selected for the Xen hypervisor, Xen can benefit from built-in integration with the kernel-based IPTables firewall. Xen's security architecture is also well documented; however support for Xen is limited.

6.2 Hardware Consolidation

The primary driver for organisations considering virtualisation is hardware consolidation and utilisation. While virtualisation offers the possibility of extensive savings in terms of hardware costs, it is important not to lose sight of the security, availability and management implications of consolidation. Consolidating too many physical servers onto a single hardware platform can create difficulties segmenting the network, creating single points of failure in a previously highly resilient system.

6.3 Logical Topology

Virtualisation increases the divergence of the physical and logical topologies, with almost every layer of the network capable of being virtualised onto a single platform. When designing a virtualised environment, ensure that the physical and logical topologies are well understood in order to minimise the time and cost of supporting the environment.

6.4 VM Spread

One of the major risks of virtualising an environment is that it becomes so easy to create new virtual machines that the spread of new virtual machines across the network can get out of hand. This makes management difficult, as well as potentially causing security vulnerabilities when virtual machines are deployed without proper consideration.

It's therefore important to update your security and deployment policies to take into account the ease with which new virtual machines can be configured and deployed, and ensure that the security implications for each new virtual machine instance are well understood and potential vulnerabilities mitigated.

6.5 VM Migration

Most Enterprise class hypervisors allow VMs to move to different physical hardware platforms in response to hardware load and failures. While this can greatly improve the responsiveness and availability of a virtually hosted service or application, it's also possible to completely circumvent your carefully configured security architecture if VMs can migrate across platforms with different security controls.

7 Approaches to Securing the Virtual Data Centre

The challenges of securing a virtualised data centre need not be a barrier to reaping the full benefits of a virtualised infrastructure. The following measures can be used to ensure that you maintain or enhance the security of your data centre infrastructure when moving to virtualisation.

- **Hypervisor firewalls:** as the network layer becomes virtualised within a hypervisor, it is important to maintain segmentation between hosts on the same hypervisor. VM migration can pose a challenge to maintaining segmentation: the logical answer to this is to move the firewall into the virtual network itself. A number of solutions exist, including the use of IPTables in Xen environments, as well as commercial firewall solutions for VMWare environments. At the time of writing, there are no hypervisor firewall solutions for Hyper-V.
- **Hypervisor IDS/IPS:** in a similar way to hypervisor-based firewalls, a hypervisor based IDS/IPS can monitor inter-VM traffic on a single hypervisor, ensuring that malicious traffic can be detected and blocked.
- **Virtual Firewalls:** traditional firewall vendors are reacting to the move towards virtual infrastructure by creating virtual firewall appliances. Although these appliances do not exist at the hypervisor level, it is possible to deploy firewalls on a per-physical platform basis. Care should be taken to ensure that the virtual network layer is configured in such a way as to ensure that traffic passes through the virtualised firewall.
- **Host based IPS (HIPS):** moving the security perimeter on to the host level allows a much more flexible environment where machines (virtual or otherwise) can protect themselves from threats using heuristic-based analysis and central management.
- **Virtual Switching:** virtual switches, like the Cisco Nexus 1000V, integrate and replace the hypervisor virtual network layer, and allow enhanced configuration of the network layer between hosts on the same hypervisor. This allows the deployment of traditional segmentation and security techniques within a virtual environment.