

NLAWARP White Paper Number 1

Data Handling and Encryption

Introduction

A number of recent events have heightened awareness around a range of Information Security measures. This white paper the first of a series, to be produced through the National Local Authority WARPs (NLAWARP) initiative and supported by BeCrypt, will explore some of the issues and offer basic advice to Local Authority practitioners.

Background

Socitm recently produced a set of guidance called the top Ten tips for Data handling, a simple framework which covers the governance and policy issues relating to Data Handling. The UK Government technical authority CESG, has also released guidance for Government departments. This paper explores three areas, the top 10 tips for data handling, a summary of the government guidance and some good practice notes around data security.

Achieving data confidentiality

Achieving confidentiality of data is a straightforward process with encryption, and technology is available today to enable this to happen. Solutions that are transparent to the user and therefore minimise the impact on how the user works are available that can provide an assured level of confidentiality. However an appropriate process needs to be defined and communicated to ensure its successful use. Data can be copied onto removable media and encrypted, but then the question of access is raised. To whom and how should the data be made available?

This has been particularly important in the cases of government offices, for example, where confidential data is increasingly required to be shared with external agencies and third parties. The data can be encrypted and transferred to the third party, but a process needs to be in place that defines who should be able to read the data. If a process is not put in place, then the encryption technology runs the risk of not being deployed.

Shared secrets

Mechanisms are required in the process whereby there are 'shared secrets' in place between organisations that have a requirement to share data. In the absence of pervasive PKI, these secrets may be encryption keys, passwords or pass-phrases. These need to be agreed with partners and support a process for data to be exchanged with confidentiality, enabling those that require access the ability to do so.

With a traditional focus on confidentiality within the Information Assurance community, rules and procedures surrounding the sharing of keys have often been

so restrictive as to threaten the availability of a system. If it is overly complex for organisations to share keys, the choice is often: ignore security, or risk data not being available.

With a growing focus on risk management in recent years, products assured for government use have been able to incorporate simple mechanisms to help solve problems such as key sharing .

The growing requirement to encrypt removable data has driven this development, as the exchange of electronic data is increasing, both in frequency and volume. This is itself posing a challenge. It is difficult for individuals to appreciate the enormity of the risk and exposure that might ensue from the loss or theft of one piece of media and its contents. Faced with a three foot high stack of paper documentation giving confidential details – home addresses, bank codes – an individual would appreciate that the information requires a high degree of protection and security. However, if this information is transferred to a disk it takes a considerable mind leap to apply the same requirement for security to one or two CDs.

Getting the right balance

Security is just one part of the puzzle. The usability of the data is determined by getting the right balance between three elements – confidentiality, integrity and availability. Buying the security technology is not enough, there needs to be understanding and action as to how it is employed. Clearly educating the users about the importance of the process is vital and ultimately, reduces the risk that the system will not be used. If good understanding of the process is in place, this will complement the technology and contribute to its overall success.

Technology can also ensure compliance with processes to protect data. This allows organisations to be more accountable for electronic assets and provide a policing mechanism that makes it more likely that people will comply, by either controlling or monitoring behaviour.

Ensuring Compliance

A port control solution is designed to secure a desktop or laptop computer from the introduction of unauthorised data (including software, music and graphical images), and from the accidental or malicious leakage of data via Plug and Play devices such as removable disk drives, MP3 players, and printers.

Such a solution enables data security to be controlled centrally, enforcing the business defined policies on the end users. Typically, groups of users can be set up on the system so that each group is subject to the most appropriate level of security – for example the Finance Group may be able to access some data via a USB port, while a support department may never need to use data from the network and so the USB ports are effectively ‘locked down’.

This type of system also provides an audit of activity. If files are copied onto a memory stick this is recorded, enabling a data leak to be quickly located and identified.

Availability is key to success

There is no doubt that data protection is becoming of increasing concern, both to large organisations and the individual. Indeed, identity theft at the level closest to home occurs with personal details thrown away in discarded post.

The new NHS national patient record system highlights potential risk at an even higher level. Yet again, the confidentiality applied to the system needs to be balanced with availability. It is important that if rigorous security controls are applied to medical health records, their availability and integrity are paramount.

Systems are available that provide an alternative approach to supporting distributed data and systems. Rather than widely replicating data, secured media can be used to provide remote access to shared data and systems.

Companies need to carry out a risk assessment from the outset - how and with whom is data to be shared and exchanged? What are the implications of the theft or loss of this data? What impact do security mechanisms have on other aspects of the system? Has a process been defined to ensure balance?

Clearly such questions should address the three key elements: **confidentiality, integrity and availability**, not just within the organisation but with partners.

Companies that achieve the right balance with the deployment of both technology and policies will be successful in ensuring that their data is secure, yet accessible to the right users.

Socitm's Top Ten Tips for Data Handling

- **Ensure you understand which legislation affects your business area.**
- **Ensure a named individual in the business owns the risk, not ICT.**
- **Ensure there is an effective incident reporting mechanism in place**
- **Regularly monitor, measure and audit your processes and procedures**
- **Implement a Corporate Information Governance group.**
- **Ensure all staff are trained, update and aware of their responsibilities**
- **Undertake regular risk reviews of all processes and procedures.**
- **Ensure all key Information assets are classified and are resilient**
- **How robust risk driven processes in place for "ad Hoc" situations.**
- **Have documented policy driven processes and procedures in place**

BeCrypt's Seven Point Plan for Successful Deployment of Data Encryption Solutions

- Decide policy ie. who has access to what data, and what can be shared with outside organisations
- Put processes in place to ensure that the policy can be maintained and staff understand both the policy and the processes they need to follow
- Define simple "Shared Secret" procedures to share information with external organisations.
- Ensure there is balance between keeping data secure, whilst enabling those that need it to have access.
- Ensure that both data integrity and policy is maintained by making the processes easy to use through the use of technology
- Educate users to recognise the enormity of risk involved with digital assets and ensure people take responsibility for their actions.
- Use technology to audit that people have complied with the procedures.

besafe.besure  becrypt

NLAWARP PO Box 6733 Chingford, London E4 8UD Tel: 020 8524 2185
www.nlawarp.gov.uk Contact: mark.brett@socitm.gov.uk

BeCrypt Limited, Wyvols Court, Swallowfield, Berkshire, RG7 1WY
Tel: 0845 838 2050 email: info@becrypt.com www.becrypt.com

© 2008 Copyright of this document is owned jointly by Socitm and BeCrypt.

Non-Commercial and Public sector organisations may reproduce the contents of this document, so long as the source and copyright owners are acknowledged.