

Removing the complexity from information protection

How encryption can add value to your business

July 2009

With data breaches widespread, no organisation can afford to be complacent, but most data losses are avoidable. Many of the breaches making headline news are caused by the loss or theft of laptops and other portable devices. To protect themselves from financial and reputational damage, encryption technologies can reduce risks by ensuring the information on such devices is secure when users are on the move. They can also add value by allowing the secure sharing of information among authorised users and by enabling more secure remote working.

Fran Howarth
Quocirca Ltd
Tel : +31 35 691 1311
Email: fran.howarth@Quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: +44 118 948 3360
Email: clive.longbottom@quocirca.com



An independent report by Quocirca Ltd.

www.quocirca.com

Commissioned by WinMagic

© 2009 Quocirca

quocirca

Removing the complexity from information protection

How encryption can add value to your business

The use of encryption is no longer optional for many organisations. Certain new regulations demand its use while others provide a safe harbour so that organisations do not have to notify individuals in the event of a security breach—provided data was encrypted. Even those organisations that are not subject to such regulation should consider the use of encryption as best practice for protecting data on portable devices.

- **Security breaches are everyday news**
Data is increasingly being lost through theft and carelessness. As mobile devices proliferate and become ever smaller, more powerful and functional, it is all too easy for such devices to go missing. This puts large amounts of potentially sensitive information at risk.
- **Encryption, and specifically full-disk encryption, is coming into wider use as a security best practice**
Software-based full-disk encryption and newer self-encrypting hard drives provide the highest level of protection by ensuring that no data can be retrieved by third parties from devices that have been lost.
- **Encryption adds value to an organisation by enabling the secure sharing of information**
Data security technologies should not restrict access to useful information. Rather, the use of encryption allows authenticated users to more easily and securely share information and enables organisations to expand their mobile working practices in a secure manner.
- **Organisations can use encryption to considerably reduce risk across their organisation**
By ensuring that encryption is always on, is transparent to the user and cannot be bypassed, the chance for human error is reduced considerably. For the best benefits, organisations should look for a product that integrates with all existing technologies in use, including security technologies such as threat management systems, all operating systems and all devices.
- **Encryption can aid organisations in achieving their regulatory compliance objectives**
Through the use of full-disk encryption, organisations can ensure that no information, such as file names remain in the clear, so saving the expense and possible embarrassment of having to notify individuals in case of the loss of personally identifiable information. The use of self-encrypting hard drives and trusted hardware devices that can be safely erased adds a further layer of protection and can reduce the cost of securely repurposing old devices for new uses.
- **Productivity gains will be seen through ease of deployment, management and use**
Provided the right solution is implemented, through centralised management capabilities, encryption software, cryptographic keys and security policies can be easily deployed and managed, freeing up IT resources for other tasks. Users will also benefit through robust self-service capabilities for provisioning encryption keys and resetting forgotten passwords.

Conclusions

The complexities and cost of using encryption systems have been reduced considerably through the provision of centralised management, making the use of encryption viable for organisations of all sizes. Whether centrally managed on-premise or through a hosted service provider, full-disk encryption systems can shield organisations from data loss and help them achieve their security objectives.

1. Introduction: why data gets lost

Losses of sensitive information by organisations make headline news on an almost weekly basis these days. According to the Privacy Rights Clearinghouse, more than 262 million data records containing personally identifiable information have been compromised through security breaches in the US alone since January 2005. Such losses occur for a variety of reasons, including criminals hacking computer networks to get their hands on information that can be used for commercial gain, carelessness by computer users in terms of sending out sensitive information in unprotected communications or losing computational devices, and deliberate security breaches caused by disgruntled employees. Many of these data losses are avoidable.

The majority of organisations have responded to external threats such as hackers by implementing security controls in an attempt to lock down their networks. These include the deployment of technologies such as firewalls and virtual private networks, and by ensuring that security vulnerabilities are patched in a timely manner.

However, data published by Data Loss DB, a data breach clearing house, regarding data breaches that were made public in 2008, shows that just 14% of data breaches were caused by hackers. This compares to more than 32% that resulted from the loss or theft of laptops, mobile phones, or other portable media and storage devices.

Many of these devices are used routinely to process, communicate and store sensitive information such as customer lists, sales records, human resources information or financial details. The majority of organisations today face some sort of regulation that demands that controls are put in place so that data is stored and communicated securely. Some of the most recent regulations go a step further and require an organisation that has suffered a data breach involving personally identifiable information of living persons to publicly notify those affected that their information

“In the future, where losses of laptop computers occur and where encryption software has not been used to protect the data, enforcement action will be pursued.”
The Information Commissioner’s Office

could have been compromised. The first such regulation was put in place in California (SB 1386)¹ but today most US states have enacted similar legislation, as have many countries around the world. In the EU, authorities can already take action against data breaches under data protection laws and amendments to the e-Privacy directive (2002/58/EC)² were made in May 2009 that makes breach notification mandatory for internet service providers should a breach such as theft of a list of customer data occur. Further amendments are likely.

However, there is at least one caveat in most of these regulations—if the data that was lost was encrypted in an acceptable manner, it is considered that the data is secure and no public disclosure of the data breach is necessary. Even where regulations do not demand it, encryption of sensitive information on easy-to-lose mobile devices such as USB drives and DVDs should be considered to be best practice and is increasingly being recommended by public and private bodies alike.

For example, the Information Commissioner’s Office (ICO) of the UK has recently ruled that three National Health Service trusts were in breach of the UK Data Protection Act because of the theft or loss of laptops or USB memory sticks that had no encryption applied to them. As a result, the ICO has issued guidance stating that all organisations should ensure that laptops or other portable devices used by organisations to store personal data should be encrypted. In the US, encryption of all portable computational devices is mandatory for federal government agencies (Office of Management and Budget M-06-16)³ and the Cabinet Office in the UK has also recently introduced similar measures⁴.

This report discusses the different types of encryption available for protection against data breaches and provides recommendations for end-user organisations as to what they should look for when evaluating a system. This includes discussion of new types of encryption devices and services both available now and coming onto the market. Key attributes that will influence the success of any implementation are ease of deployment and use, and the ability to protect data stored on any type of portable device in use.

2. Take control of critical information

Main findings:

- Threat management technologies and user awareness training should be used to provide protection against hackers looking to steal information
- Identity and access management tools control who is accessing sensitive information, and can be used in combination with strong authentication for extra security
- Data loss prevention controls can be used to restrict users from sending sensitive information out of an organisation
- Quocirca recommends that encryption technologies are utilised to protect information on portable media to prevent information falling into the wrong hands should a device be lost or stolen

• Controls against hackers

Organisations today use a plethora of technology applications to run their businesses—and a wide range of security controls for protection. When it comes to data security, there is a dizzying array of choices. Some of the best known technologies and those that are in the widest use are threat management technologies such as anti-malware, intrusion detection and prevention technologies, as well as firewalls. These can help organisations protect themselves against exploits caused by malicious software being installed on systems by hackers, which aims to steal data such as email addresses, passwords and credit card numbers through such exploits as key-logging activities. User awareness is also key in preventing malware infecting networks by making the employee aware of the dangers of malicious exploits and by educating them as to what behaviour is expected. Measures to take can include prohibiting actions such as the removal or bypassing of security controls that the organisation requires to be installed and used. These requirements must be set out in the organisation's security policy, which must be communicated to all employees and its provisions enforced. Security awareness training must also educate employees as to how to respond to other types of security exploits, such as social engineering events (for example, "phishing" attacks) that try to trick users into giving away information such as passwords.

• Placing controls on users

Identity management and access control tools are also important in controlling who has access to what information in an organisation. Such tools ensure that computer users can only access the data to which they are entitled, with access controls tied to both a person's individual name and to their role in the organisation. In order to control those entitlements and to ensure that any changes in a user's position or employment status are reflected in access rights, entitlements given should be tied to organisational directories, such as Active Directory or other LDAP directories that are used as the central store for information about users and their identities. Such integration also allows organisations to leverage the policy management and enforcement controls built into such systems, such as Active Directory Group Policy.

Alongside this, processes must be put in place to authenticate individuals trying to gain access to the corporate network before the device is able to boot up and reach any network resources. At the simplest level, users can be provided with a user name and password combination. However, such "challenge and response" security is not seen as being a secure enough practice for many organisations and the risks of easy to guess or poorly stored passwords are only too well known.

For providing greater security in access control and authentication procedures, strong authentication tools such as security tokens or smart cards provide the added assurance that the person trying to gain access to network resources has a physical token that has been issued to them. In the majority of cases this will incorporate a one-time password as an extra credential. For situations where even stronger authentication is required, access can be controlled based on something unique to an individual, such as a fingerprint biometric which can be authenticated using a USB stick, smart card or a reader residing on the device through which the person is authenticating.

- **Placing controls on data**

In most organisations, data resides in four main states: stored on stationary devices, stored on mobile devices, in transmission over networks and printed on paper. Over the past couple of years, new products have come onto the market that are a combination of tools for protecting such content from leaking out of the organisation. Such tools are known as data loss prevention (DLP) products and are designed to detect and prevent the unauthorised use and transmission of confidential information, whether deliberately or inadvertently.

DLP products enable an organisation to discover what data is on which devices such as desktops, laptops and other computer equipment to provide visibility into where content is stored and to secure or even relocate that data to a more secure location. They can be used to monitor and report on all usage of data, including where they are transferred, and can be used to block any files from being copied, emailed or even printed if the activity is deemed to be in contravention of security policy, such as prohibitions against the transfer of highly sensitive information. With these capabilities, organisations will be in a position to know exactly which information has been transferred to portable storage devices as well. Should an organisation suffer the loss or theft of a portable device, DLP tools can help an organisation to recover from the loss as, through monitoring all files and activity associated with the device, they know what information is contained on the device and can thus look for an alternative source of the information.

Thus, DLP tools, in combination with other security technologies described above, have an important role to play in protecting sensitive information by preventing employees from sending the information out of an organisation, be it by email, instant message or on portable devices.

- **Use encryption technologies for protecting information on portable devices**

However, there are many legitimate cases where an organisation wishes its employees to carry sensitive information on portable devices. Many employees and executives today travel routinely and need access to information without the requirement to always log in remotely to the organisation's network to access the information needed. People also routinely work from home or a client location and wish to take information with them on laptops or portable storage devices. Should those devices be lost or stolen, the data on those devices could be read by those who have found or taken them—if the information they contain is left in clear text. For ensuring that such information is secure, the answer is to encrypt data on all portable devices so that they do not become an avenue for data theft. This will also shield organisations from the need to notify individuals that their personally identifiable information may have been compromised should such a security breach occur, as well as preventing theft of other information, such as valuable intellectual property.

3. Different encryption offerings available

Main findings:

- Full-disk encryption provides the broadest level of protection for portable devices and ensures that, should a device be lost or stolen, no data can be retrieved from the device involved
- Selective encryption provides secure access to shared drives and disks, enabling the secure sharing of information by allowing secure collaboration
- The introduction of self-encrypting devices and the development of the Opal standard by the Trusted Computing Group will drive greater adoption of encryption

Encryption is a method used for protecting information by applying algorithms to data so that the text is scrambled and therefore unreadable by anyone who does not have the correct key for unscrambling that data. Encryption can be applied at a number of levels, from encrypting data in motion across networks to data at rest on disks. For encrypting data on laptops, other mobile devices and removable media, there are primarily two choices—encryption of the entire disk, which is considered to be device-centric encryption, versus individual files/folders or container encryption, where the focus is on specific items of data.

- **Full-disk versus selective encryption**

Of these two choices, full-disk encryption provides the greatest security against data loss should the device be mislaid or stolen and should therefore be considered to be best practice. This is because it encrypts almost everything on the disk, including file names, temporary files, boot sectors and the swap space, with the exception of the master boot

“SUVA understood that encrypting all data would not only prevent unauthorised access to a client’s personal information via a lost or stolen laptop, but would also conform to the requirements of the Swiss data protection laws.”

Jens Albrecht, CEO, SUVA

record (MBR), which must be left unencrypted in order for the drive to start up. This is especially important to prevent data loss as unencrypted sectors of disks can reveal confidential information, such as temporary files. Also, full-disk encryption ensures that users cannot bypass the system—files have to be saved encrypted, as there is nowhere on the disk to save anything unencrypted.

File/folder and container encryption has conventionally been used for encrypting small parts of a device, such as document files or folders containing several files. Using these encryption methods, different cryptographic keys can be used for different parts of the disk, meaning that access rights could be given to a particular user for a limited portion of the information. This type of encryption is particularly useful for access to shared drives, especially on a network.

However, the prime disadvantage of selective encryption is that these systems do not generally encrypt such things as file names and sizes, or metadata associated with documents. This is an important distinction because a great deal can be

ascertained just from the name a file is given with regard to discerning what its content might be. If an organisation were to lose a laptop or memory stick on which some files were encrypted, but the associated file names were left in the clear, they could still suffer embarrassment if someone finding the device were able to see that it contained information such as the payroll of its employees and publicised that loss. After all, the use of information involved in a security breach for nefarious purposes has not been proved in the majority of cases. Just the fact that the data has been lost is enough to tarnish corporate reputations and potentially lead to lost business. Therefore, file/folder encryption should be used in addition to full-disk encryption where required—not as an alternative. Thus, a hybrid system can be created in which all data on drives is encrypted to provide ultimate protection, but more granular levels of access can be granted for some files, so that access rights to those specific files can be granted only to authorised users.

- **Software-based versus hardware-based solutions**

Traditionally, encryption products have been software-based, which has the advantage that the technology can be used for existing devices in use across an organisation, including laptops, removable media and servers.

More recently, manufacturers have started offering self-encrypting hardware, in which the encryption is performed by a cryptographic chip on the hard drive itself in a secure, tamper-proof partition for pre-boot authentication. Increasingly, software encryption vendors are offering support for hardware-based encryption devices through their central encryption management systems since such devices need an activation agent and the drives need software to manage them. This has advantages in terms of transparency of encryption and performance over software-based encryption methods. The disadvantage is that hardware encryption cannot be retrofitted to legacy devices, meaning that it is only available for new devices purchased. Therefore, Quocirca advises that most organisations should pursue a hybrid policy of using both software-based and hardware-based encryption methods.

“The benefit of the Opal standard is that it provides instant security. By 2012, it will be a standard feature. All drives shipped will have an encryption engine.” Mike James, senior director, Fujitsu

In early 2009, the Trusted Computing Group (TCG) released its Opal Security Subsystem Class Specification⁵, which is a storage specification intended as a blueprint for manufacturers wishing to develop self-encrypting hard drives. This will drive interoperability and will allow organisations to mix and match drives from different vendors. Opal specifies the minimum acceptable core specification capabilities of a storage device tailored for PC clients and data centre storage devices, including how data is locked, how encryption keys can be erased, and how they are integrated with Trusted Platform Modules for safekeeping of identity credentials.

The Opal standard

The main purpose of the Opal standard, released by the Trusted Computing Group in January 2009, is to address the issue of data at rest to provide protection against offline attacks. It is applicable to devices ranging from desktops to storage systems, including USB sticks. The other main use case for Opal is that it is intended to allow secure repurposing of end-of-life equipment. In this case, drives can be quickly sanitised as the cryptographic key used to encrypt the data can simply be deleted, making it virtually impossible to recover the data.

According to Jorge Campello of Hitachi and Chairman of the Trusted Computing Group, which developed the Opal standard, "Data loss is an ever-increasing problem. There have been solutions before, but they were always proprietary. Opal provides the standardisation needed. But it is not a point solution and it is not just for storage vendors. The most important factor for the success of Opal and self-encrypting drives is that the system is managed by the right software to centrally manage the user interface and passwords, and so on. Therefore, encryption software vendors must embrace the standard."

Over time, more and more hardware products are expected to be equipped with self-encrypting capabilities, which will help to expand the use of encryption. A further benefit of self-encrypting devices is that they can be more easily and cheaply repurposed, allowing organisations to get more from their investments. As the data held on such devices is already encrypted, devices can be safely moved between employees, with the recipient being able to "reformat" the drive through using a new encryption key, but not to see any of the original data held on the device.

However, there is controversy as to whether the content on such drives should really be considered protected because only the encryption key has been erased. Some feel that if you cannot access that data, it is as good as erased—which should be good enough for a lost or stolen device. When a device is to be repurposed, a new encryption key is generated and new data overwrites the old.

However, others, including the US government, believe that just using software designed to overwrite data is not a viable enough data destruction solution, especially for data deemed to be confidential or top secret, when a device is to be repurposed. Guidelines issued by the US Department of Defense (DoD 5220.22-M)⁶ that are applicable to all government employees with regard to the handling of classified information state that, as of October 2007, overwriting of data is no longer enough for the sanitisation of magnetic media such as disk drives. Only degaussing (erasure through magnetisation) of such drives is acceptable. However, this does not account for solid state drives, which are coming into wider use. These devices cannot be degaussed as they are not magnetic media, meaning that secure erase is the only option for reuse of such drives at this point, or device destruction to prevent any reuse at all.

Another recent development is the provision of hardware-based encrypted USB sticks that can be defined as trusted devices. Many such USB devices available on the market will provide an extra level of security by self destructing the encryption key if a series of attempts are made to read data from the drive without following the proper decryption method. However, a secure mechanism is provided for recovering encryption keys from central repositories so that data can be recovered.

4. Encryption as a business enabler

Main findings:

- Ease of use is of paramount importance for any encryption deployment
- Central management capabilities automate key processes and ease the burdens associated with deployment and ongoing management
- Use of encryption should be combined with strong authentication for higher levels of security
- To reduce risk, any encryption system should natively integrate with other technologies in use in the organisation
- New, hosted, software-as-a-service models extend the benefits of encryption and strong authentication to organisations that lack the resources or will to manage a system in-house

• Ease of use is paramount for enabling productivity

A key factor in any technology implementation, and security in particular, is that it must be easy to use so that employees are not hindered in doing their work. To ensure that encryption is easy to use, it should be transparent to users. They should never be confronted with having to make a choice over which encryption algorithm to use—or indeed whether or not to use encryption. Since full-disk encryption scrambles all data on a device, it can be thought of as hardware-level, or device-level, encryption. By locking down everything on a drive, the computer user does not need to make decisions as to which information should be encrypted and what can be left in the clear.

Once full-disk encryption has been installed on a device, all data written to that drive is automatically encrypted, and when files are read from the disk, they are automatically decrypted. This means that all encryption and decryption procedures are transparent to the user and there is no action required on their part to ensure that all data is secure when the device is powered off. This makes full-disk encryption especially important as a security tool for protecting portable devices and can be an enabler of remote working, which has many implications for the productivity of the workforce.

“Once a disk is encrypted, it acts just as it did before it was encrypted. It’s almost like SecureDoc isn’t even there.” Andrew Labbo, The Children’s Hospital

Modern encryption systems generally provide online self-help capabilities that can aid employees since they can immediately obtain the help that they require should a problem be encountered, such as a forgotten password, or a lost security token or smart card. Through these capabilities, users can more easily and quickly regain control of an encrypted laptop or other portable device, without having to call the helpdesk to gain access to the resources that they need to carry on working.

• Ease of deployment and management reduce administrative burden

To ensure that encryption is easy to deploy, administer and manage, any product chosen should have a centralised enterprise management server to reduce the burdens of deployment and management. In the majority of products, this is supplied as a console that is installed on standard servers equipped with a standard underlying database. Through integration with other functional components in use in an organisation, this console provides the administration and management capabilities needed to automate all tasks for deploying encryption to users. For example, through integration with Microsoft’s Active Directory or other LDAP directories, security policies related to encryption can be deployed and enforced and granular levels of access can be granted to users and groups according to role based on user profiles that already exist.

Case study: The Children's Hospital, Denver

Founded in 1908, the Children's Hospital in Denver (SickKids) has been treating children for more than 100 years. Today, it has a new hospital, opened in 2007, a network of 13 care centres and 400 outreach clinics throughout Colorado. It employs more than 1,000 paediatric specialists and more than 3,000 full-time employees.

Because it is so geographically dispersed, its medical staff needs to travel between facilities and needs access to patient records at each location, requiring them to travel with laptop computers, which are a mixture of Windows and Mac machines. Patient records are deemed highly confidential and must be protected when held on a laptop under the requirements of the Healthcare Insurance Portability and Accountability Act (HIPAA) so that they cannot be accessed if the laptop were lost or stolen.

In line with these needs, SickKids began researching full-disk encryption products. Whilst it was conducting this research, an incident occurred that underscored the importance of encrypting portable devices and lent a certain urgency to the search for a solution. The key features that SickKids looked for included integration with Microsoft Active Directory, centralised management capabilities, a robust and secure backend, reliable and secure key management, support for various operating systems, user friendliness, and compatibility with existing technological environments in terms of both hardware and software.

SickKids began its encryption implementation with two pilots, testing to see if full integration was possible with existing technologies and how well the management software worked. The pilots confirmed that all their requirements were met and that no data was lost during installation of the system.

Today, SickKids has deployed WinMagic's full-disk encryption to all of the laptops in use by the hospital and also configures the encryption software to perform automatic encryption of removable media if requested by the laptop user. Where sensitive data needs to be transferred among staff, USB keys with built-in hardware encryption are provided to users.

According to Andrew Labbo, privacy and data security officer and information security manager for SickKids, "When you compare the relatively tiny cost of protecting each laptop to the potentially high cost associated with a single user losing their data, it is remarkable that every organisation is not protecting their data in this fashion. Installing encryption software makes perfect sense from both a data security and a return on investment perspective."

A central management server can also ease headaches surrounding one of the most problematic areas of encryption—that of key management. Effective management of cryptographic keys is essential because the point of using full-disk encryption is to prevent data loss, but the easiest way of losing data forever is to lose the key that can decrypt that data. This means that any encryption tools chosen should provide strong key management capabilities in terms of user provisioning and de-provisioning according to policy and user rights, storage, and backup capabilities for encryption keys, including secure escrow. Should a device that has been encrypted be lost or not returned, the system should also be able to destroy the keys associated with that device to ensure that no one could ever recover the data on that drive.

The benefits of centralised management are that the time taken for setting up the system and for ongoing administration and management are reduced dramatically, freeing up network and systems administrators for other tasks. Users will also benefit from the provision of online self-service capabilities that allow them to more quickly reset forgotten passwords or request replacement security tokens, which also frees up helpdesk resources and reduces the cost of administration further. All of these factors will aid an organisation in improving productivity.

- **Combine with strong authentication for more robust security**

For providing greater security in access control and authentication procedures, any encryption solution should provide support for strong authentication tools such as security tokens or smart cards. The use of smart cards for pre-boot authentication has further advantages for controlling access in that they can be extended to other environments, such as being coupled with physical access controls for gaining entry to buildings or parking garages. Such use of smart cards for combined logical and physical access control has been boosted by the development of the Federal Information Processing Standards (FIPS) specification 201 as part of the requirements of the Homeland Security Presidential Directive 12, which mandates the use of identification cards using encryption and strong authentication methods for all federal employees and contractors needing physical access to government facilities and logical access to computer systems. This standard is coming into widespread use in the US government and similar schemes are being implemented in countries worldwide based on the standard, which is boosting the use of strong authentication cards for physical access. The standard provides for protection against internal and external security breaches but, when combined with pre-boot authentication, that protection can also be extended to prevent unauthorised access to stolen laptops.

When deciding what security tokens to use, organisations should look closely at the regulations that their business faces, as many demand that robust security controls be applied for data security. In many cases, government security certifications are coming into wider usage in the private sector as they provide assurance over the quality of such factors as the encryption algorithm used, key management capabilities and international recognition. For disk encryption solutions, FIPS, specifically FIPS 140-2⁷ and Common Criteria⁸, are the main standards that attest to vendor commitment to best practices for security. Their adoption is especially important for organisations that work with or supply to the public sector since they will be required to support such standards as they are often mandated for use by many governments. Even those that do not should look to adopt these standards as the basic foundation for their own security.

“The price of a laptop itself is insignificant when compared to the value of the data, so you want to be sure that unauthorised users cannot gain access to valuable information via a lost or stolen device.”

*Damon Allen, Manager,
distributed systems operations,
Arch Chemicals*

In many cases, organisations will wish to provide users with access to shared drives on the network or folders transferred among users on portable drives such as USB sticks. Through integration with directory controls and by assigning the right to groups of users to share an encryption key, organisations can actually allow users access to resources on a shared drive, folder or USB stick in the knowledge that only those with authorisation to do so can access them. When they try to access the drive, the server checks with user directories to see whether or not they have been granted permission to access that drive. These checks are done in a manner that is transparent to the user since they won't see the background restrictions that are in place. In this way, removable media can provide added value to the organisation by enabling users to share information in a secure manner. For example, executives working on a merger and acquisition plan may wish to share those plans among themselves, whilst ensuring that those that are not involved in the deal cannot gain access to such sensitive information.

- **Integration with existing technologies improves security**

Another feature of encryption systems that can make them complex to manage is that they must interface with other technology controls in an organisation. Therefore, organisations should look for systems that natively support a wide range of technologies commonly in use in an enterprise, including firewalls and threat management applications, without the need to make any changes to the existing network architecture.

Organisations should also look for systems that work across all platforms and operating systems, which may include Linux, UNIX, Mac and various mobile device operating systems, as well as Microsoft platforms, since most networks employ a range of technologies. Support should also be provided for multiple versions of operating systems, such as Windows XP, Vista and 7, including both 32-bit and 64-bit versions. Database and directory support is another factor to look for in a system, including support for standard databases such as SQL, along with Active Directory and other LDAP directories for tying access rights to identities.

In order to ensure that support is provided for all data at rest in heterogeneous technology environments, the encryption tools should not only encompass all applications and platforms, but also all devices that are used for connecting to the network. This should include personal computers, Macs and servers, as well as portable devices including laptops, mobile phones, trusted devices, self-encrypting hard drives, CD and DVD drives, and any generic USB flash memory stick. Only through support for all technologies and devices used in an organisation can enterprise-wide data security risks be comprehensively managed.

Case study: Arch Chemicals

As a biocides company, Arch Chemicals is used to keeping bad stuff at bay. Taking approximately US\$1.5 billion annually in sales, Arch provides chemistry-based products for controlling the growth of harmful microbes in water, hair and skin products, treated wood, paints and building products, and health and hygiene applications. It employs around 3,000 people in operations centres dispersed throughout the world.

Because it is so geographically distributed, many employees need to travel extensively, requiring that they are equipped with laptops—a couple of which are lost or stolen every year. To prevent any of those losses resulting in a data breach, Arch began looking for an encryption solution to safeguard the data. However, Damon Allen, Manager Distributed Systems Operations, who was placed in charge of looking for the solution, was aware that encryption is the type of technology that users find daunting to use. As Allen states, “We wanted to be certain that the encryption software would not only meet all security and management criteria, but would also be so transparent that data would be protected without the user really having to do anything.” Other key objectives were that the solution was easy to administer and that it would help them not only to meet, but to surpass, all requirements for compliance with privacy and other regulations.

Arch underwent a three-month pilot to evaluate encryption offerings, concluding that the SecureDoc technology from WinMagic provided the best combination of security, ease of use and ease of administration on the market. According to Allen, “I had previous experience in a lawsuit where someone wanted information from a laptop. The laptop was protected with SecureDoc, and the recovery company could not bypass the encryption. That type of scenario gave me real confidence in the encryption capability of the product.”

Today, it has rolled out the product to 800 users worldwide, who are served by a 24-hour help desk for resetting forgotten passwords. Deployed in one central location, the system is administered by one IT person in each geographic location where the solution is deployed. In this way, staff from China to the US can be helped whenever a problem arises.

According to Allen, Arch Chemicals has stringent and ever-more-demanding security requirements and understands that data protection is a critical part of doing business. “A data breach can be catastrophic so you need to be 100% certain that all data on all devices is protected at all times,” states Allen, adding that SecureDoc has met every one of the organisation’s security requirements and given him great confidence that all information is protected at all times, no matter where users travel.

- **Provision of lower cost business models**

The centralised management capabilities provided by enterprise encryption systems can do much to reduce the associated costs of administration and management of encryption. However, some organisations are extremely resource-strapped and may consider that encryption could best be provided as a service by an organisation with the relevant expertise. This is especially true of small and medium-sized organisations, or those with just a small number of remote workers who are in just as much danger of losing mobile devices or having them stolen as any other organisation.

Encryption vendors have started offering hosted models, offering encryption as a subscription-based service. This provides access for a monthly fee without the need for upfront investments.

To meet the needs of such organisations, some encryption vendors have started offering encryption services based on a subscription-based, software-as-a-service (SaaS) model. As with annual licence fees, subscriptions are generally based on the number of users, but the monthly subscription basis of most contracts offered by vendors, or their service providers who are hosting the service, means that the number of users can be scaled up or down as required in a SaaS or hosted model.

The use of hosted or on-demand encryption services provides many of the benefits of enterprise deployments for securing data against loss. These include automated policy and key management, and the provision of centralised reporting and audit capabilities for achieving compliance with regulations, including those relating to privacy and data breach

notification. Subscribing to hosted services that cover encryption needs, not just for desktops and laptops but also all sort of portable devices, will help organisations ensure that as many data sources as possible are brought under management and so enhance security for the mobile workforce. To ensure that workers stay productive, organisations must look for strong self-service capabilities through provision of a web-based interface for such needs as forgotten passwords.

5. Benefits of the use of encryption for mobile devices

The benefits of using encryption—and specifically full-disk encryption—are numerous. Not only do organisations protect themselves from potential fines and reputational risks but they are able to achieve goals such as compliance with privacy and data protection regulations. Further benefits brought through use of encryption are that such technology can actually add value to the organisation by enabling higher levels of productivity for both administrators and users, as well as enabling secure remote working, which further raises productivity.

The following table summarises some of the main benefits for use of encryption systems for organisations:

<i>Benefits of encryption</i>	<i>How encryption helps organisations to achieve their goals</i>
Increased value	<ul style="list-style-type: none"> • Use of encryption can help organisations achieve goals such as compliance with privacy and data protection regulations through reporting and auditing of all actions taken via the central management server • Central management capabilities enable higher levels of productivity for both administrators and users • Full-disk encryption enables increased levels of secure remote working
Reduced risk	<ul style="list-style-type: none"> • Full-disk encryption provides protection from potential financial losses and reputational harm by eliminating the need for security breach notification when a device is lost • By making encryption transparent, always on and impossible to bypass, users are not faced with a choice of whether to use encryption or not • Reduced risk of customer dissatisfaction through the ability to shield customer information to reduce the chance of identity theft or financial fraud occurring
Lower cost	<ul style="list-style-type: none"> • Centrally managed encryption provides reduced total cost of ownership for the encryption system through the provision of tools for making administration easier • New technologies are coming on to the market that allow full-disk encryption to be extended to a wider range of devices with little or no extra cost • With full-disk encryption, the loss of a device becomes just that—the loss of something costing a few hundred Euros, rather than the high cost associated with recovering from a data breach

6. Conclusions and recommendations

Once seen as expensive and difficult to use, encryption systems on the market today solve many of the complexities of data security at an affordable price. They can also help an organisation to improve the productivity of those administering and using such systems, reducing the risks that the organisation faces. The table below provides a checklist of some of the key areas of functionality that is recommended that organisations should look for when selecting an encryption product set.

Encryption, and specifically full-disk encryption, technologies can help shield an organisation from data losses through loss or theft of mobile devices such as laptops, mobile phones and other portable media, which are coming into greater use in all walks of life. Through integration with all data sources and existing technologies in use, and by tying access control and authentication to enterprise directories, organisations can use encryption to protect data throughout the enterprise.

As well as reducing risk, the use of encryption can add value to an organisation by enabling more secure remote working and sharing of information, and by helping organisations to achieve regulatory and business compliance goals, and in particular those related to privacy, data protection and security breach notifications.

For those unwilling or unable through lack of resources to administer and manage the system by themselves, new hosted solutions are appearing on the market. With such solutions, a third party service provider performs all tasks required centrally, with users accessing the system through a web-based portal or mobile device. Users can be kept productive through provision of a 24x7, web-based, self-service portal to keep them working even when they have lost a security token or forgotten a password. In this way, organisations of any size can reap the benefits that using encryption brings, without having to make any upfront investments in technology.

Recommendations: What to look for in an encryption solution

Provision of multiple types of encryption solutions

Integration with authentication and access controls

Support for strong authentication tools

Provision of pre-boot authentication capabilities so that the solution can be extended to other environments, such as the use of smart cards provided for physical access controls as well as authentication on devices and the network

Support for recognised standards

Support for mobile phones and other portable media and storage devices

Encryption should be always on, transparent to users and impossible to bypass

Centralised management capabilities for provisioning users and for policy management and enforcement

Robust cryptographic key management capabilities

Provision of self-service capabilities for users

Integration with existing technologies and security controls in use in the organisations

Support for all operating systems and types of devices in use in the organisation

Highly secure backend controls and provision of a failover server for disaster recovery purposes

7. References

¹ SB 1386: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

² 2002/58/EC: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>

³ Office of Management and Budget M-06-16: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>.

⁴ Cabinet Office final report on data handling procedures in government:
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

⁵ Opal Security Subsystem Class Specification:
http://www.trustedcomputinggroup.org/files/static_page_files/B1105605-1D09-3519-AD6FD7F6056B2309/Opal_SSC_FAQ_final_Jan_27_4_.pdf

⁶ DoD 5220.22-M: <http://www.dtic.mil/whs/directives/corres/html/522022m.htm>

⁷ FIPS 140-2: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

⁸ Common Criteria: <http://www.commoncriteriaportal.org/thecc.html>

About WinMagic

WinMagic provides the world's most secure, manageable and easy-to-use data encryption solutions. Compatible with all editions of Microsoft Windows Vista, XP, and 2000 as well as Mac and Linux platforms, WinMagic's SecureDoc™ protects sensitive data stored on portable media such as laptops and removable media including USB thumb drives and CD/DVDs. Thousands of the most security conscious enterprises and government organizations around the world depend on SecureDoc to minimize business risks, meet privacy and regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over three million SecureDoc users in approximately 43 countries. For more information, please visit www.winmagic.com, call 1-888-879-5879 or e-mail us at info@winmagic.com.

SecureDoc, SecureDoc Enterprise Server, Compartmental SecureDoc, SecureDoc PDA, SecureDoc Personal Edition, SecureDoc RME, SecureDoc Removable Media Encryption, MySecureDoc, MySecureDoc Personal Edition Plus, MySecureDoc Media, and SecureDoc Central Database are trademarks of WinMagic Inc. Other products mentioned herein may be trademarks and / or registered trademarks of their respective owner.

Contact:

Joseph Belsanti

Vice President, Marketing

Joseph.belsanti@winmagic.com

+1 905 502 7000 x221



WINMAGIC[®]
DATA SECURITY



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank WinMagic for its sponsorship of this report and the WinMagic customers and partners who have provided their time and help in the preparation of this report.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption—the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O₂, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>