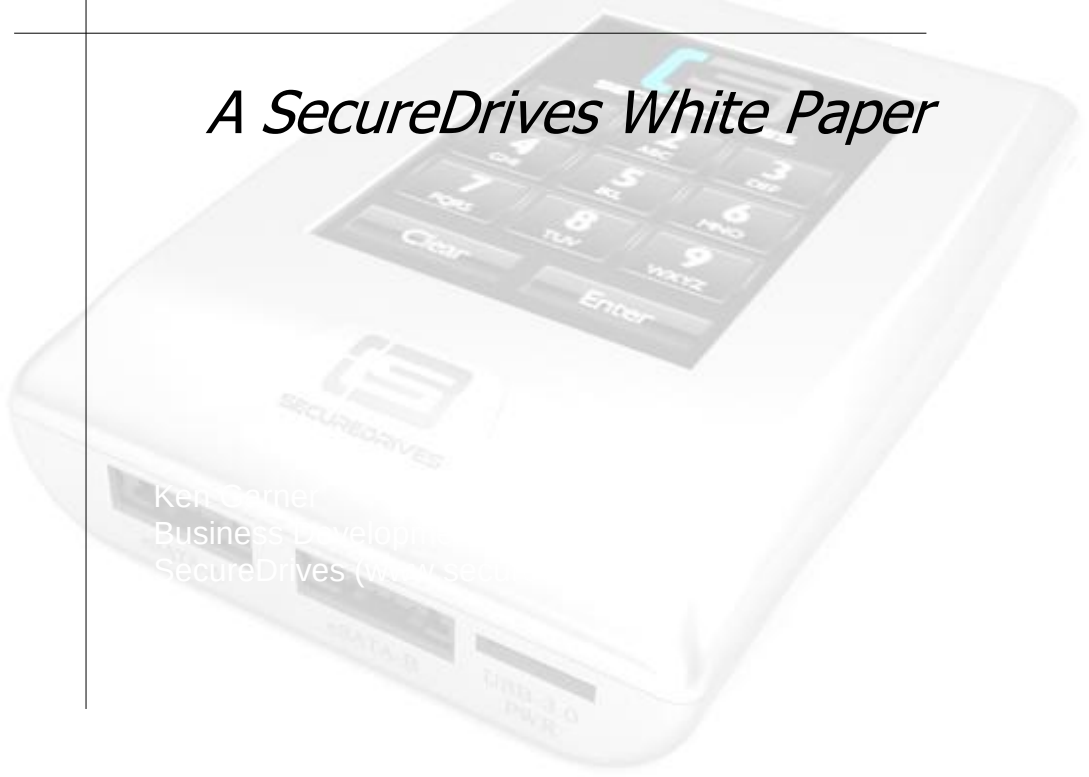
SECURITY BY DESIGN

A SecureDrives White Paper



Ken Cornell
Business Development
SecureDrives (www.securedrives.com)

January 2011

Contents

List of Figures

Purpose and Scope

This SecureDrives white paper is designed to provide an up-to-date understanding of the UK and international regulatory and data security threat landscape together with an overview of workflow problems and logistical issues surrounding current data encryption and automated backup technology. The paper will focus in particular on the problems associated with sensitive data which has to be stored securely by end users at the point of use and regularly backed up. This paper explains the SecureDrives solution and is aimed at personnel who are responsible for implementing, performing or reviewing information security processes, managing data loss policies, developing supply chain compliance strategies and supervising non-technical data users.

Introduction

Access to up-to-date information delivers competitive advantage. Technology makes information readily accessible and available to share, within the enterprise, with clients and suppliers and throughout the extended domestic and international supply chain.

Sharing information increases productivity, but at the same time storing sensitive company or personal data raises issues about accidental data loss or the misuse of sensitive confidential data by third parties.

The data threat landscape is changing very rapidly. The UK Information Commissioner has recently gained new powers of entry and inspection without notification.[1] Provisions introduced earlier this year in the 2008 Criminal Justice and Immigration Act will enable the ICO to impose substantial fines on organisations where there is evidence of reckless or deliberate data protection breaches.[2]

The Information Commissioners Office (ICO) is also re-defining their existing powers under the Data Protection Act (DPA) 1998.[3]

Recent ICO adjudications have reinforced the principle that the provisions of the DPA 1998 take precedence over any existing policies, standards, accreditations or prior working practices.[4]

At the same time cybercriminals are mounting sophisticated, highly targeted automated attacks using techniques derived from internet grooming to target companies of all sizes who might hold valuable or sensitive data.

Recession induced layoffs also places data at risk. Remaining, often overstretched staff, begin making mistakes with data, putting company reputations on the line.

Because we live in a world where everyone, everything, everywhere is connected, data has to flow to and be stored wherever it is needed; an organisations actual perimeter is no longer its physical or legal boundary.

---

[1] The press release announcing these new powers can be viewed at *http://www.ico.gov.uk/upload/documents/pressreleases/2008/statement_new_powers.pdf*

[2] The CJA 2008 can be viewed at http://www.justice.gov.uk/news/newsrelease090508b.htm

[3] A summary of the DPA 1998 can be viewed at http://www.ico.gov.uk/what_we_cover/data_protection.aspx

[4] A summary of recent adjudications is at http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

The security focus is moving away from the network edge and onto the end point and the data user with the spotlight firmly on encryption and automated backup as the only sustainable, affordable and workable solutions. Encryption addresses three main business issues. It reduces the risk of data loss. It helps companies comply with legal and professional regulatory requirements and encryption builds trust by demonstrating a company's commitment to data security.

Most companies will have data security policies already in place ranging from Acceptable Use Policies, Information Protection Policies, HR Policies and Employment Contracts. Many will also have contractually imposed Information and IP protection safeguards imposed by upstream suppliers and downstream customers.

However a significant number of information security breaches come about as a result of employees' failure to comply with existing, well documented, security practices and policies. Many organisations have tried to sustainably modify user behavior towards data security and encryption. Almost all have found it difficult.
Research has shown that most of these data security breaches are caused by security mechanisms which are either technically complex or have become an impediment to the user completing their work in a timely fashion.[5]

Even technically competent users such as systems administrators and software developers often struggle to keep up with the ever increasing complexity and administrative workload created by GRC, DLP and security and encryption processes.[6]

The goal has to be to provide "practical security" using encryption tools which non-technical end users can operate correctly with little or no training, which have minimal impact on existing network infrastructure and working practices and which work within a borderless organisation where work and leisure time are becoming increasingly blurred.[7]

Issue	Effect
Incompatible Systems	Data cannot be encrypted and freely exchanged increasing risk of data loss
Complex and technical	User workflow is interrupted and productivity is decreased, many users find a workaround.
Manual generation of passwords	Slower business process, risk of insecure passwords or passwords being transmitted "in the clear" compromising data security
No end user authentication	Data can still get into the wrong hands
No audit or tracking	Who is or isn't using encryption?
No password expiry	The data is at risk ad infinitum
No data destruction	The data is at risk ad infinitum

Figure B.7-1. *Main Encryption Compliance Issues*

[5] Whitten, A. & Tygar, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999, Washington 1999.

[6] Yee, K P. (2005) User Interaction Design for Secure Systems. In L. Faith Cranor & S. Garfinkel [Eds.]: Security and Usability: Designing secure systems that people can use 2005. pp 13-30. O'Reilly Books.

[7] Zurko, M. E. & Simon, R. T. User-Centered Security. New Security Paradigms Workshop 1997.

SecureDrives are a unique solution to the problem of employee resistance to using encryption in that there is no software to install, little or no training is required, no changes to current IT systems or infrastructure are necessary and there are no changes to current, established working practices or workflow.
SecureDrives achieve this by balancing usability and security with productivity and compliance.

How Do SecureDrives Work?

The basis of the SecureDrives solution is a seamless blending of five separate technologies:

- Solid State technology
- Encryption
- Automated Backup
- Remote Data Destruction
- GSM

SecureDrives are a specially packaged Solid State Drive (SSD) which contains, embedded within it, everything necessary to encrypt, decrypt, backup and securely destroy sensitive data.
SecureDrives have the ability to communicate securely with the SecureDrives server.
It is the SecureDrives server which manages the generation of encryption keys.

The Data Owner/User connects the SecureDrive to his laptop. Any files copied to the drive are automatically encrypted and compressed and written into a secure storage area on the SecureDrive.

Later The Data User Reads Data On The SecureDrive. The SecureDrive contains everything the data user needs to be able to decrypt and access the data contained in the secure storage area. Every step is automated and reading a SecureDrive does not require any additional software to be loaded onto the data users' machine, no training is required, no changes are needed to the data users IT system. The SecureDrives system is designed to integrate into industry standard office workflow practices.

- A SecureDrive contains all the software needed for every stage of the data life cycle. Encryption, Decryption, Backup, Destruction.
- AES encryption
- Fully compliant with the UK Data Protection Act
- Remote data destruction
- Secure tamper proof case
- A non-technical, printed "How To" guide is included with each SecureDrive
- Secure destruction at end-of-life.[8]

[8] Password Research Institute. Improving password security and authentication. http://www.passwordresearch.com/papers/pubindex.html.

What Protection Is There If A SecureDrive Is Lost Or Stolen?

- All the data on a SecureDrive is stored in a secure storage area or data vault.
- The encryption software used is always the most up-to-date version of the AES 256 encryption standard.
- The high strength password is never revealed.
- The remote destruction feature destroys the data and the physical drive.
- If the drives case is compromised the data and the drive are destroyed
- Low battery level triggers self-destruct protecting the data.
- GSM signal starvation triggers data and drive destruction.

UK And International Compliance.

SecureDrives can help to maintain compliance with a number of UK and international legislative requirements, information security standards, industry regulatory bodies and supply chain demands. The table in Figure B.7-2 shows just a sample of the many areas SecureDrives assists with Governance, Regulation and Compliance (GRC).

Compliance Issue	SecureDrives & Zero Touch Backup
UK Data Protection Act 1998	Meets the Information Commissioners requirement for verifiable encryption.
European Data Protection Regulations	Provides compliance with Article 17 of Directive 95/46
Individual US state data protection laws	Meets all current individual US state laws
PCI DSS	Conforms to the Payment Card Industry Data Security Standard (PCI DSS) for the encryption and protection of archived cardholder data.
Sarbanes-Oxley (SOX)	Provides data protection, audit and management reports as required under SOX
HIPAA	Delivers full conformity with HIPAA mandatory encryption of medical record files plus verifiable audit trail and reports.
ISO 27001/ISO 17799	Ensures ongoing compliance with sections 10.8.0 to 10.8.5
CobiT and ITIL	Compliance via link with ISO 27001/ISO 17799
Lexcel (UK)	Helps conformity with Lexcel 4A.2
UK Code of Connection (CoCo)	Helps maintain compliance with Sections 2.10 and 2.23
Other International Jurisdictions	SecureDrives provide compliance in most other international jurisdictions, see note below and page 5

Figure B.7-2. *Compliance Issues and SecureDrives*

For more information about other international data protection jurisdictions visit:
http://www.accurateinformationsystems.com/docs/International_Data_Protection_Laws.pdf
See also http://datalossdb.org/us_states and http://datalossdb.org/us_federal_bills

SecureDrives and European Jurisdictions.

Across Europe there are over 100 country specific public bodies devoted to ensuring that sensitive personal information held within computer systems or on computer devices, or transmitted across networks, is not accessed by or distributed to unauthorized individuals or agencies. All are tasked with ensuring that national laws transposing the European Directive on Protection of Personal Data are upheld; imposing obligations on public institutions, businesses and other organizations to protect personal data. Implementation of European directive varies from jurisdiction to jurisdiction but encryption is the common denominator. As an encryption solution SecureDrives meet the personal data protection standards of all the following regulatory bodies.

Country	Agency	Website
Austria	Data Protection Commissioner	http://www.dsk.gv.at/
Belgium	Privacy Protection Commission	http://www.privacy.fgov.be
Bulgaria	Personal Data Protection Commission	http://www.daits.government.bg
Cyprus	Data Protection Commissioner	http://www.dataprotection.gov.cy
Czech	Personal Data Protection Office	http://www.uoou.cz
Denmark	Data Protection Agency	http://www.datatilsynet.dk/
Estonia	Data Protection Inspectorate	http://www.dp.gov.ee/
Finland	Data Protection Ombudsman	http://www.tietosuoja.fi/
France	Data Protection Authority	http://www.cnil.fr
Germany	Data Protection Commissioner	http://www.bfdi.bund.de/
Greece	Data Protection Authority	http://www.dpa.gr
Hungary	Data Protection Commissioner	http://abiweb.obh.hu/abi/
Iceland	Data Protection Authority	http://www.personuvernd.is
Ireland	Data Protection Commissioner	http://www.dataprotection.ie
Italy	Data Protection Authority	http://www.garanteprivacy.it
Latvia	Data Inspectorate	http://www.dvi.gov.lv/eng/
Liechtenstein	Data Protection Unit	http://www.llv.li/amtstellen/llv-sds/
Lithuania	Data Protection Inspectorate	http://www.ada.lt
Luxembourg	Data Protection Commissioner	http://www.cnpd.lu
Malta	Data Protection Commissioner	http://www.dataprotection.gov.mt/
Netherlands	Data Protection Authority	http://www.dutchdpa.nl/
Norway	Data Inspectorate	http://www.datatilsynet.no
Poland	Personal Data Bureau	http://www.giodo.gov.pl/
Portugal	Data Protection Commission	http://www.cnpd.pt/
Romania	Data Processing Supervisor	http://www.dataprotection.ro/
Slovakia	Data Protection Office	http://www.dataprotection.gov.sk/
Slovenia	Information Commissioner	http://www.ip-rs.si/
Spain	Security Secretariat	http://www.mir.es/SES
Sweden	Data Inspection Board	http://www.datainspektionen.se/
UK	Information Commissioner	http://www.ico.gov.uk

New EU Data Breach Laws.

At the January 2011 ENISA (http://www.enisa.europa.eu/) conference in Brussels is was announced that new European wide data breach regulations will be introduced under an amendment to the 1995 EU Data Protection Directive.

At the conference all of the European data protection regulators registered very strong calls for this mandatory breach notification to be applied throughout all member states and to all sizes of business including SMEs as soon as possible.

The Executive Director of the ENISA Prof. Udo Helmbrecht said at the conference:

"Gaining and maintaining the trust of citizens that their personal data is secure and protected is an important factor in the future development and take-up of innovative technologies and online services right across Europe."

In order to become and remain secure, and protect sensitive data from loss or theft it is vital to have both data security and data backup/recovery solutions in place and regularly used.

At the same time that UE wide data breach laws are forcing businesses to secure any stored sensitive data and report data breaches, other regulations require all businesses to maintain accurate financial and trading data for long periods of time and to make this data available should the authorities, or in some cases the courts, require it.

Most SMEs probably don't have the time, energy or in-house technical resources to devote to maintaining a secure system or deploy data breach reporting systems within a fast changing governance, regulatory, compliance and cyber threat landscape.

SecureDrives provide small to medium sized businesses with a simple, reliable and quick solution that eliminates the workflow friction normally associated with data security and automated backup and lets them get on with running their business.

SecureDrives and PCI DSS

Payment Card Industry Data Security Standards or PCI DSS are the industry data security regulations which govern how anyone who accepts payment cards whether in their business premises or online, via their website, must process and store sensitive cardholder data.

The regulations apply to cards issued under the Visa, MasterCard or Amex brands.

Any data breach which includes payment card data, whether hard copy or electronic has to be reported to the PCI authorities. If the data loss occurred as a result of the regulations not being applied correctly then the business can, and probably will lose their merchant status and be unable to offer payment by credit card.
Serious breaches can incur substantial financial penalties, in addition to any additional financial penalty which might be imposed by the national data regulator.

The PCI DSS requires you to:

- Apply a number of specific controls, or safeguards.
- Produce and maintain documented policies and procedures
- Apply a number of technical IT and network configurations.
- Provide staff with appropriate training
- Undertake quarterly scans.

At the same time that PCI DSS is forcing merchants to secure any stored card holder data other regulations require all businesses to maintain accurate financial and trading data for long periods of time and to make this data available should the authorities, or in some cases the courts, require it.

SecureDrives radically redefine PCI data security. As the world's most secure Solid State Drive our patented design guarantees that unauthorised person will not be able to access your customers payment card data even in the unlikely event that your SecureDrive device is lost or stolen.

Designed on the principle that lost or stolen data is unusable when destroyed, SecureDrives SSDs physically destroy the information stored on each chip – either when tampered with, or remotely at the owner's request – rendering the data impossible to recover.

Add to this an ultra-secure and randomly generated AES 256-bit CBC encryption key, constant GSM monitoring, true zero touch backup capabilities, a dedicated device management control service and you've got the only SSD that meets PCI DSS and all data security legislation within the EU.

SecureDrives work seamlessly with all operating systems from the minute you switch on and ultra-fast eSATAp and USB3.0 ports transfer data at speeds of up to 132MB/s. Zero Touch Backup Docking Pods allow faster-than-ever encrypted data transfers between external drives without the need to press a single button.

The Economics of Compliance

SecureDrives have been designed and engineered from the ground up from the individual end users point of view. It's mainly individuals who cause data loss, it's individual end user behavior which has to be sustainably modified and it's individuals who choose whether to comply or not with the security policies governing their immediate work context.

Individuals choose whether or not to comply with security guidelines based on risk and reward or cost and benefit. There is a natural limit to the amount of effort users will expend on compliance unless there is a corresponding benefit.

Modern digital encryption came out of the US military in the 1970s and 1980s.
The inflexible command and control structure of its original development environment created the encryption structures and landscape we see today.
Within a fully integrated public or private organisation, with a standardized IT structure, encryption offers nearly unbreakable information security. It's possible to demonstrate mathematically that it is computationally impossible to retrieve encrypted data without the encryption keys.

However even within a tightly integrated IT environment everyday practical issues in the deployment, maintenance and use of encryption technology have limited the business benefits and impaired the efficiency of business operations. Misapplied encryption increases risk, decreases security, incurs unnecessary costs and reduces efficiency.

Until recently it has been almost impossible for non-technical end users, with dissimilar I.T. skills and differing attitudes to data protection to securely store, use and backup confidential or personal data. This was especially the case where data was only likely to be accessed very infrequently or even on a one-off basis. The investment in infrastructure, training and skills outweighed the benefit of deploying companywide encryption technologies.

How SecureDrives work.

Unique data storage drives based on SSD technology with remote data destruction capability on demand. External and internal 2.5inch SSD drives.

Data protection process

1) Hardware level 256bit AES CBC (Cipher Block Chaining) encryption NIST (FIPS-140-2 certification pending)

On unauthorised data access detection or remote data destruction request the devices will execute the following data destruction process within mille seconds:

1) Change of the original unique device generated encryption key
2) Creation of a one way cipher key with which the partition table is re-written
3) System ICs are then destroyed via a close proximity impulse wave which results in the physical fragmentation of the SSD chips and other system components that prevent access to stored data.

External device data protection mechanisms

1) Case intrusion detection – data destruction
2) PIN code retries exceeded – data destruction
3) GSM signal starvation – data destruction
4) Battery level low – data destruction

Internal device data protection mechanisms

1) Case intrusion detection – data destruction
2) SATA Interface monitoring – Removal of SATA connector data destruction
3) GSM signal starvation – data destruction
4) Battery level low – data destruction

Highly configurable for differing level of security required

1) PIN code length
2) PIN code retries before data destruction
3) Monitor internal battery life (If battery falls below a certain level data destruction will occur)
4) Monitor for GSM signal presence (Period of time without GSM signal before data destruction)
5) SATA interface monitoring can be turned on and off via the web

End User Benefits

1) A fast SSD Drive that offers the latest data interface connectors of eSATAp and USB3.0.
2) Zero Touch Backup (ZTB) facility where the unattended backup of one device will occur when connected to a secondary device. Simply connect the two devices and a complete backup will occur via the eSATAp port.
3) GSM Location Report is available should you lose your device and want to gain a rough idea of its location. This is via the web and uses GSM triangulation to give you a rough location of the device.
4) Lost or stolen device then via the web you can request the device to destroy itself
5) For the ultimate data security make the device your bootable drive to your laptop via the USB3.0 or eSATAp port. (Laptop dependent). You then can easily backup your entire laptop drive via ZTB.
6) Desktop docking station allows you to keep your desk clear and provides a holder and power supply to your drive
7) The Zero Touch Backup docking pod provides and elegant way of holding your secondary drive and allowing for easy docking of your primary device and instant backup whenever is required
8) Stylish and the ultimate in secure data storage.

Conclusion.

In an increasingly tough business climate organisations have to decide how to spend their resources in the most effective way to achieve their operational goals.

It's important to protect client information, but the resources an organisation can deploy on information security are limited.

These limited resources have to be targeted to protect the most serious risk which is the exposure of unencrypted sensitive personal information.

Traditional encryption is unwieldy and the compliance cost is often greater than the benefit.

SecureDrives are an encryption solution which automates and deskills the entire encryption/decryption process within a cost effective, secure, workflow based environment. The SecureDrives system provides integrated zero touch backup and secure destruction at end of life.

For more information contact SecureDrives at www.securedrives.com