



BOOLE™

s e r v e r

Data Centric Security:

Ensuring Security Is More Than Just Compliance



WHITEPAPER

Not Protectively Marked

Andrew Lintell and Malcolm Gardner
© SecureGrade 2010/2011. Version 1.21

INTRODUCTION

Recent years have seen an explosion in the volume of electronic data produced and relied on by business and it continues to grow. The IDC forecast study¹ predicts that data volume will increase tenfold over the next few years, itself a significant increase over the previous period. Data management challenges facing businesses are not just related to volume, but also to the nature of the information and its importance the company itself and the regulatory attention it receives.

The conflicting goals of data availability and security are also a consistent theme, particularly when applied to sensitive and high value information. High value data can contain a wide variety of confidential information that have specific value to the organisation such as earnings sheets, product designs, customer payment details, patent information and so on. Data files often require different levels of access and security, related to the inherent value and sensitivity of their content.

Compliance, both regulatory and voluntary, is an increasingly important requirement. Modern standards, like ISO 27001, require a Security Management System to be implemented that is based on an assessment of risk and for technology and process to be applied to mitigate these risks.

However, not all data is the same. Information that is of high value to companies, but is not subject to regulatory pressures like the Data Protection Act, is often overlooked. This information can be of such high value that its compromise could have major financial or public relations implications and possibly disastrous consequences for the company.

UNDERSTANDING DATA TYPES

When considering the different scenarios within which sensitive data are used, and the risks inherent in these scenarios, it is important to understand the different types of sensitive data an organisation has. A recent Forrester study² examined the type and value of enterprise documents that contained intellectual property, and found they formed two groups.

Secrets: valuable confidential data such as financial reports, design documents, product roadmaps.

Custodial Data: data held on behalf of others such as banking data, patient data, legal contracts etc.

The value of each group differs due to the nature of their use and requirement. Proprietary company secrets generate revenue, increase profits, and maintain competitive advantage. Custodial data such as customer, medical, and payment card information has value because regulation or contracts make it embarrassing if compromised and costly to rectify.

¹ *The Diverse and Exploding Digital Universe*, IDC. March 2008

² *The Value of Corporate Secrets*, Forrester. March 2010

Table 1: Examples of Custodial and Secret Information

	Custodial Data	Secrets
Creator / Owner	Business Partners Customers	Enterprise
Relationship to data	Custodian	Owner
Examples	Customer PII Credit Card Numbers Governmental Identifiers	Trade secrets Strategic plans Sales forecasts
Source value	External: determined by regulators and criminals	Internal / External competitive
Compulsion to protect	Controlled by regulation, statute or contract	Would cause strategic harm
Regulation	DPA PCI-DSS	-
Consequences	Clean up, notification costs Reputation	Revenue losses Reputation
Key Question	Why is the data circulating?	Who needs to know?
Priorities	Stop unnecessary circulation Reduce use	Control circulation Reduce abuse

Based On: Forrester Research, "Selecting Data Security Technologies," December 2009.

INCREASING REGULATORY AND COMPLIANCE PRESSURE

Recent changes to the Data Protection Act came into force in 2010 and are designed to deter data breaches. The Information Commissioner's Office (ICO) is now able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The power to impose a monetary penalty is designed to deal with the most serious personal data breaches and is part of the ICO's overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

This drive for regulatory compliance has specific resonance for data that fall within the custodial group, however secret data remains unaffected, is company specific, arguably of higher value and has higher consequences should it suffer a breach or leak.

It is also worth noting that increasingly competitive markets and sophisticated customers are putting pressure on companies to implement, and be assessed against, non-mandated standards like ISO 27001. Customers are becoming more aware and demanding that suppliers conform to recognised standards as they themselves become more attuned to the risks inherent in sharing their own data.

COMPLIANT DOESN'T MEAN SECURE

Understanding and recognising the different types of data a business makes use of can help to address the balance when formalising where data security investments are needed. Often a company will focus on trying to prevent accidents with custodial data, due to regulatory pressures, but an additional and often overlooked risk is theft of sensitive company secrets as they carry a far higher intrinsic value.

Company secrets are the data asset “crown jewels” and represent the most sensitive activities from research and development, patent filings, mergers and acquisitions, financial and strategic direction. This information is of critical importance to the future success of the organisation. Keeping it safe should be the highest priority.

As compliance is focused on the appropriate use of custodial data, solutions that operate within that remit alone are frequently too narrow in their objective and result in overlooking valuable data assets such as company secrets. When considering solutions for the protection of sensitive information, both data types should be considered and, where possible, processes combined in order to derive maximum return for the organisation.

TRADITIONAL SOLUTIONS OPERATE IN DISTINCT TECHNOLOGY AREAS

Until very recently covering data through its life-cycle involved integrating a number of point security technologies that can help secure individual stages of the data custody chain, as shown below. These individual technologies tended not to take into account the overall business process they were operating alongside and rarely gave an end-to-end solution: at some point valuable data was left exposed.

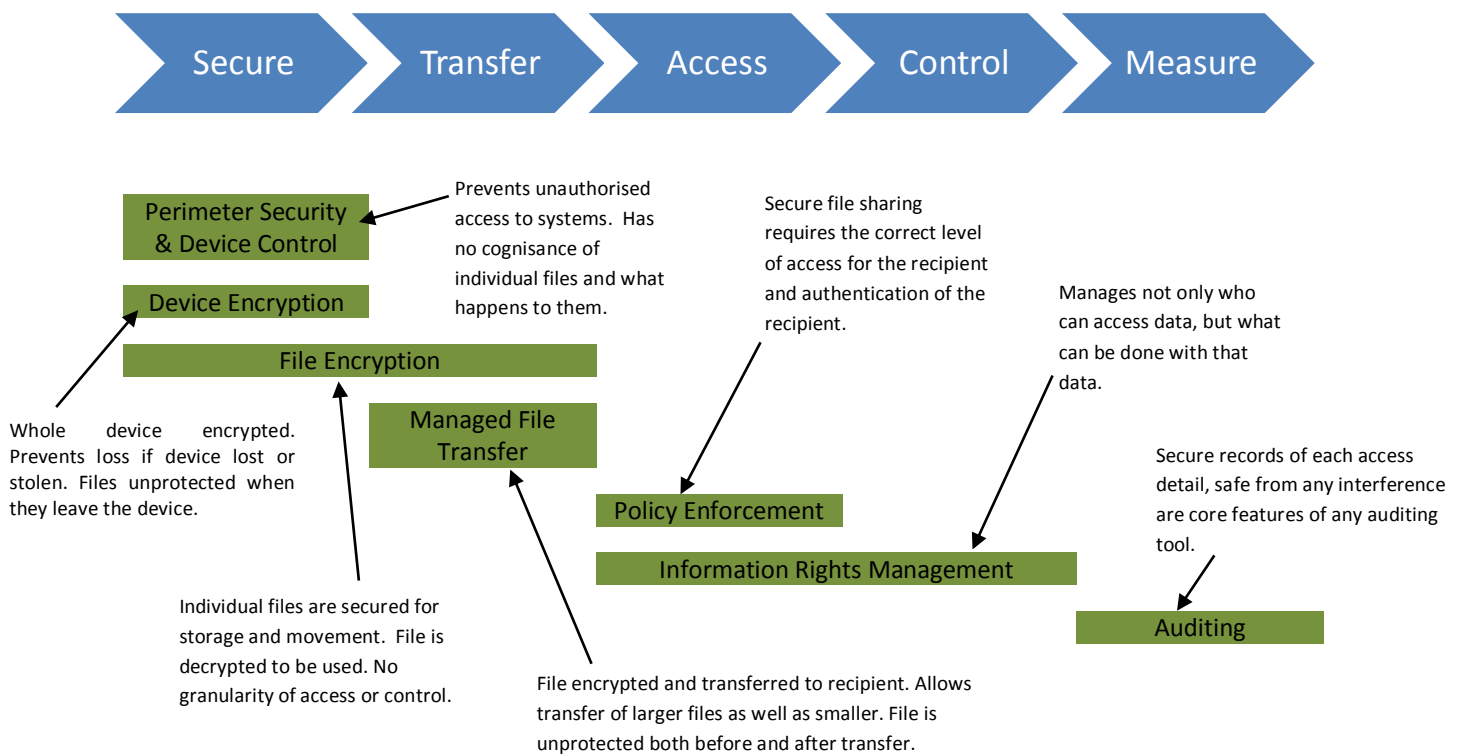


Figure 1: Traditional Technologies in the Information Custody Chain

While there are many good point solutions that operate within each of these technology areas, in combination they suffer from the same problems:

- At some point an item of data has to be unprotected in order that it can be used
- Once an item is sent out from its owner and arrives with a recipient, control is lost
- Information Security risks tend to be associated with human activity (absent mindedness leading to loss, malicious actions leading to theft, poorly designed business processes leading to compromise, etc). These activities more often than not span more than one step of the custody chain and so technology lead solutions tend to be misaligned with the risks they are trying to mitigate
- Following on from this, few of these solutions are designed to work together, creating expensive and complicated integration work or difficult to follow workflows and making it difficult to demonstrate compliance.

APPROACH THE PROBLEM FROM ANOTHER PERSPECTIVE: THINK DATA-CENTRIC

The reason that traditional solutions have the problems described above is that they focus on areas of technology, rather than starting with the higher level problem of mitigating information security risks associated with the activities of business – they are an evolution of a less mature view of security.

What is required is a security paradigm that includes the following considerations (based on the sections discussed above):

- Secure both Secret and Custodial data with the same rigour
- Secure Information irrespective of where it lies within the custody chain
- Secure Information wherever it ends up
- Remove human error where possible
- Support compliance needs
- Be driven by the needs of doing business – using but not losing data.

A recent development in this field is the concept of truly data-centric security. In this world view, individual items of data are secured irrespective of where they are held in a fashion that allows the appropriate access to the appropriate person, wherever they are and whenever they try to make access. Rights are variable by the owners of data as circumstances dictate and all actions relating to items are securely recorded for auditing purposes.

CONCLUSION

Compliance is a major spend within the security budget but does not necessarily equal secured data when it comes to sensitive information security. Enterprises need to consider placing more focus on securing critical secrets that confer long-term competitive advantage, rather than just preventing accidents involving custodial data.

By coming at the problem from a point of view that considers the business requirements that lead to information risks and selecting systems and solutions that share this world view, businesses will be better placed to support the needs of compliance and address the security of their own secrets.

Enterprises should consider data-centric security technologies that provide a unified platform to protect both types of data. They should specifically be able to accommodate unstructured information, provide the correct level of access to necessary parties and place emphasis on retaining control of information at all times including throughout any collaboration processes or sharing. Files should also be secured with persistently applied measures, allowing the file to be always protected as its minimum state, and access controlled wherever it is used, sent or stored.



Tel: +44 (0) 1582 620 613
Email: info@securegrade.com
Web: www.securegrade.com

SecureGrade Ltd
Reg No: 07211961
Postal Address: 70 High Street, Harpenden, Herts. AL5 2SP
SecureGrade is the UK representative of Sunfive S.A. the manufacturer of Boole Server.