

SECURE DATA

A GOVERNMENT CHALLENGE



Introduction	1
Rebuilding Confidence	1
Implementing “best practice”	2
Driving the Agenda	4
Leading the Initiatives	5
Conclusion	5

INTRODUCTION

Over recent months a number of high profile data losses from Government departments have been reported. Public concern is growing in the Government’s ability to handle personal information in a safe and secure way.

These concerns are being raised at a time when there is a drive to have a more ‘joined up’ Government by reducing duplication and optimising collaboration across Government departments through the use of technology. These databases are, in turn, being made available to wider audiences through data sharing initiatives. The public’s lack of confidence in the Government’s ability to look after its data is creating resistance to some of the Government’s strategic programmes. The NHS’ patient records and the National Identity Scheme are two widely publicised examples.

However, this issue is not confined to the public sector. Many private sector companies collect and manage personal and other sensitive data. Financial organisations - banks and insurance companies - are the most obvious examples but many other organisations are compiling profiles on individuals such as loyalty card operators, credit rating agencies and marketing companies. Data losses do occur in the private sector but they are less widely publicised.

This paper seeks to provide overview answers to the following questions:

1. How can we rebuild confidence around regulation based on practical experience?
2. How can good practice be identified, fostered and enforced?
3. Should the agenda be driven by industry, professions, government or regulators?
4. Who should lead any initiatives?

REBUILDING CONFIDENCE

There are no quick ways to regain confidence and trust. This can only be achieved over time and with a real and visible response to the recent highly publicised data losses

Public sector

More legislation is unlikely to assist in ensuring data safety as the reported incidents were all in breach of existing legislation. It is the Data Protection Act and Human Rights Act that provide the legal framework to safeguard privacy. Government has already introduced a new monetary penalty in the Data Protection Act (sections 55A to 55E) which has a new monetary penalty to ensure that data controllers, who do not take reasonable steps to avoid the most serious breaches of Data Protection Act principles, may be subject to a fine as well as to an enforcement notice.

New technologies such as remote encryption can certainly help. However, it is more in the area of policy and procedure that best practice will be achieved. There are mechanisms already in place:

- The Cabinet Office has set a strategic information assurance and security framework for Departments to implement;
- HM Treasury has produced and distributed corporate governance and accountability requirements;
- The Cabinet Office has produced the Civil Service Management Code;
- There are vetting procedures for employees.

In the light of recent events it is clear that these procedures are not preventing data losses.

There is, therefore, a need to have pan-government procedures that are as consistent in their implementation as they are in their content. As part of the rebuilding confidence programme there needs to be a publicity campaign that informs the public that the problem has been recognised and that Government has a programme in place to prevent future occurrences.

Private Sector

The Data Protection Act and the Human Rights Act are just as applicable to the private sector as they are to the public sector. The private sector is, additionally, driven by commercial pressures to protect personal and other sensitive data. A commercial organisation that fails to protect client information is likely to suffer financially due to any publicised data breaches or losses. Consequently, security breaches do not reach the press in the same way as the recent UK Government revelations have.

How information is stored and accessed is constantly changing and there is increasing awareness of the lucrative and illegal trade in personal data. It will, therefore, be a requirement that any mechanisms and / or legislation put in place to protect personal data are constantly reviewed and updated, not only to keep pace with issues of the day but also emerging threats.

A recent report, commissioned by Fellowes for National Identity Fraud Prevention Week, found that 97 per cent of UK consumers are not completely confident that the organisations they deal with are taking adequate steps to protect their information. Worse still, 92 per cent of employees at the firms in question confessed that the identity of their customers could be stolen by a fraudster, while 75 per cent admitted that their employers could be doing more to prevent fraud. The report authors said that their research found a remarkably complacent attitude towards the security of personal data.

IMPLEMENTING “BEST PRACTICE”

Effective security and compliance measures are essential to safeguarding personal data. Balancing this protection with the corresponding costs—both direct (the cost of the security controls themselves) and in terms of reduced productivity and business agility, is a demanding challenge and needs to be measured to achieve the necessary balance.

Historically the view has been that:

- IT security is an isolated discipline;
- Risk management is segregated by department;
- Management has a reactive response to unsophisticated threats;
- A strong perimeter / firewall is sufficient;
- Processes are disconnected with ad-hoc responses to regulatory change;
- Security and compliance are seen as a cost.

Without delving into specific cases of recent government data losses it would be fair to say that, generally speaking, these have occurred through human error and there is a clear need to educate employees in behaviour that is appropriate to support the development of policies and procedures.

What is required is a cultural change - the modern forward thinking approach recognises the risk of well orchestrated, intelligent threats that must be handled by an integrated and fully coordinated security approach, extending throughout and across the organisation. Compliance with new regulations is an adaptive, integrative process, thoroughly ingrained into daily operations.

The modern organisation's best practice policies include:

- Protection against orchestrated, intelligent threats;
- Taking an integrated and fully coordinated approach;
- Making compliance an adaptive process;
- Including risk management as part of the company's DNA;
- Being able to clearly demonstrate that personal data is adequately protected;
- Communicating those policies in a manner that can be understood by the people to which they are most relevant.

What then would a "best practice" programme look like? CSC sees three components to a data protection strategy:

1. Risk Governance,
2. Information Risk Management,
3. Security Operations

1. Risk Governance

The most strategic element, measuring where risk exists and supporting enterprise risk management by measuring the consequences of IT security decisions and improving the prioritisation of resources.

- Enterprise protection programme
- Security strategy
- Security policy development

2. Information Risk Management (IRM)

IRM defines the appropriate levels of security control required to protect the 'lifblood' of any organisation be it public or private sector. IRM activities should include:

- Information risk assessment and profiling;
- Business continuity planning;
- And compliance assurance.

3. Security Operations

Security operations manage the operational day-to-day integration of IT, facilities and personnel protection. This part of the strategy covers detection of threats, protection and response and remediation and would include a comprehensive programme of operational activities such as:

- Vulnerability management;
- Centralised user provisioning;
- Technology compliance;
- Managed authentication;
- Forensic services;
- Disaster recovery;
- Incident response;
- Wireless security,

All of the above may be provided as a managed security service.

The major benefits of implementing a structured programme means that we now have the ability to apply metrics to risk elements, quantify their value to the organisation and apply protection commensurate with the identified value-at-risk. Specific benefits include:

- Compliance is made part of business as usual;
- Security is made a cohesive whole, from policy to operations;
- A shared insight into the probable business impact of actual/anticipated security incidents;
- Understanding of the stakeholder value of information risk;
- Security expenditures aligned with business / departmental priorities and compliance imperatives.

DRIVING THE AGENDA

Nominations for the driving seat are: industry, the professions, Government or the regulators. In the long term it is the citizen / consumer that will drive the agenda. The citizen will not vote for a government and a consumer will not use the services of an organisation that does not look after their best interests.

In the short term all the nominees have a role to play. Any organisation that collects and stores personal or other sensitive data should 'own' the responsibility of protecting that data.

Industry

Industry will implement data protection procedures where it is commercially advantageous for them to do so. For example; an organisation such as Iron Mountain may differentiate itself from competitors by publicising its security features. Industry will also respond when the disadvantage of not implementing effective procedures leads to a commercial loss. This might be regulatory penalties, breach of contract or bad publicity.

Those professions that store personal information such as; doctors, lawyers, accountants and tax advisors will have similar outlook to industry.

Industry will not drive the agenda through goodwill. There needs to be a commercial interest, positive or negative, to motivate participation.

Government

Collectively government departments hold the most of our personal data. The government also has an institutional duty of care to protect the information it is entrusted with. It is the combination of these two factors that has caused the press and public to become increasingly vocal with their concerns about the collection and collation of personal details in central data repositories.

This outcry does not help the Government's plans. Firstly, it reflects badly on a government that is approaching an election. Secondly, it alienates the public from those objectives of Transformational Government which are to create efficiencies and economies through shared services and the re-use of data. For programmes such as the National Identity Scheme, resistance from the citizen needs to be overcome if it is to be adopted by the public.

Given the above, it is clear that the Government would gain the most from being seen to drive the agenda. There would be both political and administrative advantages in being seen to have grasped the issue and clearly demonstrating that it can put its own house in order. This should be achieved before applying legislation and regulation to the private sector.

Regulators

The Government looks to the regulators to make effective use of best practice. The regulators are in a good position to develop working practices which could usefully be developed as a code of regulatory best practice in managing personal data. However, there are dozens of regulators in the UK with diverse responsibilities. Developing a consistent policy amongst the full spectrum of regulators would undoubtedly be a challenge. Nevertheless the regulators would be well positioned to oversee the implementation of a process that was predefined and issued to them.

LEADING THE INITIATIVES

We have determined that Government has attracted the most attention with its recent data losses and is in need of winning support for its initiatives. What is required, therefore, is a government department or a single regulator to own a programme of assessment and amendment to win back public confidence and gain public acceptance for national programmes that involve the collection and storage of personal data.

It might be appropriate to extend the remit of the National Audit Office to include a review of current practices, identify areas of risk and report failures to meet an agreed national benchmark.

CONCLUSION

The portability of laptop computers, PDAs and other mobile computing devices makes these convenient business tools easy to steal and misplace. Memory sticks have a capacity up to 32GB, are small, easy to use and easy to lose. For these types of device, data encryption is essential. It should be assumed that the device will, at some point, be lost. The question the organisation must ask itself is; *“what is the best position I can be in when this eventuality occurs”* and then plan accordingly. A programme of encryption should be undertaken with immediate effect.

With regards to an overall strategy our recommendations would be to;

- Initiate a structured assessment of all the government departments that hold personal data to determine a profile of the data management practices and the risk levels for data loss. Create a data classification scheme in order to be able to ‘structure’ and protect data commensurate with its ‘risk value’. This approach would allow for stronger controls around that data which is considered most sensitive, whilst allowing Government and Industry to benefit from new technology in its day to day business. This assessment might be done by a number of third parties but the same process should be followed by all assessors to achieve a comparable benchmark.
- Included within the remit will be paper based data. Some of the reported data losses involve documents that have been left in public places. Policy procedures should dictate what paper based documents can and can’t leave the offices. Restricted documents could be RFID tagged so that their movements can be recorded both in and out of offices and maybe even utilising paging system triggered when the documents leave the vicinity of the carrier.
- Identify a standard that any organisation in the private or public sector should not fall below. Guidance on establishing the necessary policies and procedures to achieve a good level of security is provided by the ISO 27000 series standards.
- Appoint an assessor / regulator with the responsibility to conduct regular appraisals of all relevant Government departments.
- Once this appraisal process is established and operating effectively it should then have its footprint widened to include those private sector organisations that store personal data.

The loss of personal or sensitive data usually occurs, and is not reported, for months or years following the incident. Regulation might include a time period for reporting a data loss after which penalties would be incurred.

More information

To find out more about CSC’s services to the public sector please contact Malcolm Stirling, Director Public Sector on 07717 697889, or visit us on www.csc.com/government



Worldwide CSC Headquarters

The Americas

3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa

Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia

26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia

139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 45 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."