Business Case for Creating a SIRO Role

Background Information

1. INTRODUCTION

The 2007 HMRC CD incident and subsequent developments have brought the information assurance agenda further up the corporate agenda. The Data Protection act clearly states that organisations MUST look after personal information. The ICO now has the power to impose large fines. Councils hold vast amounts of personal data both electronic and on paper, about customers and employees, and services and properties. Proper arrangements need to be in place to safeguard this information. The importance of proper information assurance and governance, driven by a formal information risk management process, has been borne out by the number of data losses which continue to be reported across the public sector. Recently outbreaks of the Conficker virus in Councils continue to show that threats to information security are ever-present.

It is essential to have technical measures in place, such as encryption, to mitigate the risk, to have policies and procedures to dictate how these should be used and to carry out training and awareness-raising to remind staff to follow these. There is also another important element in the information security framework, namely governance. In this context this means that we must have clear responsibilities and reporting lines to ensure that information security is managed properly and that we have a comprehensive view of the state of information security across authorities.

2. DRIVERS FOR APPOINTING A SENIOR INFORMATION RISK OWNER (SIRO)

Following the loss of data by HMRC and several other security breaches, the Government conducted a review of its data handling procedures and one of its recommendations was that all Government departments should designate a board member as Senior Information Risk Owner (SIRO) and that all information systems should have an Information Asset Owner. The Local Government Association (in its *Data Handling Guidelines*, issued last year) said that all local authorities should do the same. These roles are also well established in the NHS.

As part of their Key Lines of Enquiry (KLOE), many authorities report on their approach to data quality.

In addition to these external drivers, there are other reasons for clarifying roles and responsibilities in relation to information security. As part of the GCSx Code of Connection, it is a requirement to report security incidents to GovCert UK (The CESG Computer Emergency Response Tam), and or a Local WARP Warning,Advice and Reporting Point).

Over the last few years a number of potential and actual security breaches have been reported. Some of these have led to serious consequences and have been reported to the Information Commissioner, who investigates breaches involving personal data. In such cases the Information Commissioner normally checks on the governance arrangements for information security, including whether an organisation has a SIRO. It should be remembered that the Information Commissioner

has the power to compel an organisation to improve its information security arrangements, and some councils have recently had to sign undertakings to this effect. In addition, the Information Commissioner will shortly be given powers to fine organisations that mishandle personal data.

The SIRO role will also support any initiatives to reduce risk following the investigation of security threats such as the Conficker virus.

Councils are currently stepping up awareness-raising for staff on information security and there is a need to identify resources for this. There is often someone already undertaking many of the functions required; this approach simply formalises the ad-hoc arrangements that may be in place. Clarifying the governance arrangements will help to ensure that we get the best value from this investment in the future.

3 INFORMATION SECURITY ROLES

The key roles in the governance of information security are the SIRO, the Information Security Group (ISG) and the Information Asset Owners (IAOs). All staff, members and partner organisations also have a responsibility to follow our security policies.

3.1 SIRO

Local Government Association guidance and best practice elsewhere suggests that the SIRO

- is the officer who is ultimately accountable for the assurance of information security at the Council
- Champions information security at EMT level
- Owns the corporate information security policy
- Provides an annual statement of the security of information assets for the Annual Governance Statement (as part of the audit process)
- Receives strategic information risk management training at least once a year

The SIRO is not intended to be a new post but rather a newly-defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with IT, but takes a broader view of our information assets as a whole, in any form.

Individual authorities will determine exactly where the role and responsibilities lie within the council.

3.2 The Information Security Group (ISG)

A working group set up by the Chief Officer Steering Group or Executive Management Tem to look into the state of information security in the Council. This group is composed of representatives from the Corporate Information Unit, Legal Services, Finance, CICT (Corporate ICT), Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections attend meetings as required. The ISG has developed policy and guidance on information security and piloted a reporting procedure for information security breaches.

It is proposed that a group should continue to meet and should support the SIRO. Its remit will be to:

- Develop or review an information security strategy for the Council
- Develop information security policies and guidance and ratify changes. New and changed corporate policies are to be approved via the Council's normal process (Example policies can be found on the Government Connect Code of Connection Toolkit site at: www.g3ctoolkit.net
- Assist with management of security risks in projects through the project life cycle
- Review all reported security breaches and report them regularly to the SIRO and onward to GovCert and the WARP.
- As appropriate, report information security breaches to the Information Commissioner via the SIRO
- Promote awareness of information security by all officers and Members
- Plan, develop and deliver training on information security as required

- Produce an annual statement on the security of our information assets for the SIRO, covering breaches, training, results of audits, progress made against the Information Assurance Maturity Model (IAMM), using the Information Assurance Assessment Framework IAAF) etc both available from www.cesg.gov.uk

3.3 Information Asset Owners (IAOs)

IAOs are the senior managers across the Council who are currently responsible for the main information systems and information assets. In terms of information security their responsibilities are:

- To manage security, compliance and risks associated with their information assets
- To carry out an annual assessment of information risk as part of risk management
- To ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- To ensure that information security incidents are reported via the Council's information security incident reporting procedure see www.govcertuk.gov.uk and www.nlawarp.gov.uk
- To ensure that actions are taken to remedy breaches
- To classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- To receive information risk management training annually
- To consider on an annual basis how better use could be made of their information assets within the law

In the main these are not novel proposals but rather the normal responsibilities of senior managers responsible for information systems and assets.

3.4 All staff, Members and partner organisations

All staff, Members and partner organisations that access our information must follow the Council's security policies in handling information in any form. Any deliberate breach of Council policies which compromises the confidentiality, integrity or availability of Council owned information assets may be a criminal offence for which individuals may be personally liable.

For further information contact: mark.brett@lga.gov.uk

We greatfully acknowledge the assistance of the Yorkshire and Humber WARP and Bolton Council in the production of this document.