

Focus on data security

With information technology being hailed as the key to future public sector performance, the need to address security risks has never been greater, writes **REBECCA THOMSON**

Local government's approach to data security is often ineffective, with a quarter of councils suffering a security breach in the past year, research has found. This is despite most being aware of the efficiency and service improvement benefits that technology can bring, and rating security as crucial.

A survey of senior council managers conducted by LGC and commissioned by professional services company VEGA, found that councils' approach varied considerably.

Nearly 70% of councils viewed information assurance – the process of managing and minimising the risks of storing data – as “essential to joined-up government and doing more with less”. And 75% said the connections with colleagues in other areas, such as health, were an “important” or “very important” part of having good communication.

Some progress has been made, with 81% saying they have a security policy that is widely available to staff. Two-thirds said all new staff received security training and 86% provided staff with guidance on the Data Protection Act and Freedom of Information Act.

However, 19% described information assurance as “problematic”. And although respondents recognised the importance of information assurance to keeping personal and corporate

information safe, less than a fifth made data security the responsibility of a board-level representative. A third relied on a ‘senior information risk owner’, or SIRO, and 32% on an IT security officer.

Only 39% trained board members responsible for security and risk, and only 30% said they regularly updated staff on new security practices. This is particularly problematic, experts say, because developments in this area are fairly common and new processes are always being formed. This means vigilance is required from managers.

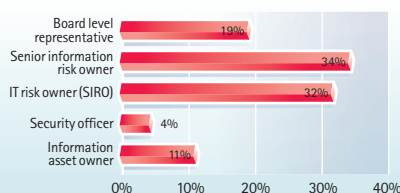
Many were also unclear on the implications of central government initiatives aimed at improving data security.

Nearly half (47%) thought better communication with central government improved their council, but only 31% were aware of the Cabinet Office's Security Framework Policy, while 41% were not aware of the Public Sector Network, which will eventually link the whole public sector via a common IT network.

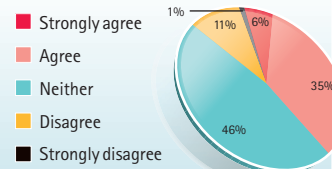
The lack of clarity surrounding central government data security projects was also reflected in the

number of councils – 59% – who said they “neither agreed nor disagreed” with the statement that government gives “appropriate guidance on

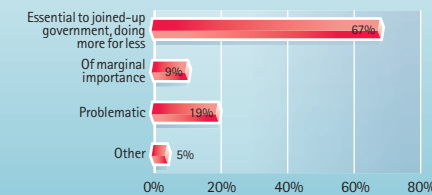
Responsibility for data security



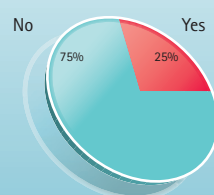
Councils that regularly receive sensitive information from government via the internet



How councils view information assurance



Councils that have experienced a security breach in the past year



information assurance”.

Over a third (35%) admitted receiving sensitive government information via the internet, despite security experts warning against the practice. And 36% of councils said they regularly received requests to send sensitive data themselves via the web to central government bodies.

Christopher Boyd, a researcher at Sunbelt Software, advises councils to have the right defences in place. “Sending sensitive information through regular internet traffic is a bad idea.

Always use secure channels to send sensitive information – use a VPN, avoid webcafés and steer clear of free webmail services to store or send data,” he says.

The difficulties are reflected in the finding that 25% suffered a security breach in the past year. In almost half of these cases the impact was felt at board level or externally in the local community.

The managers who took part in the survey agreed local government's performance on data security could be shaky. “There is inconsistency across councils generally, although in my authority it is taken very seriously,” says Diane Spencer, asset manager at Woking BC.

“In this authority each and every member of staff has been trained, and all business managers have to sign compliance statements. Others I know in different authorities have not been so vigilant,” she adds.

The results of the LGC/

More online

For the full survey results go to:

**LGCplus.com/
VEGA**

Security grows

VEGA survey confirm councils are all approaching the issue in different ways. This means some are doing well, but others don't always recognise the importance of adhering to strong policies around data management.

"It is probably true to say that staff turnover and communication issues sometimes mean that employees don't have a full understanding of the systems that are in place," says Lyn Boyle of Gateshead Council.

"When it comes down to information sharing this is where the need for protocols is vital, and this is the area where there is potential tension and where poor communication and personalities can have an impact on implementation."

It is a view shared by Paul Orłowski, VEGA's Information Security Practice Leader, who says that, as with all such change programmes, the main issues lie in cultural and training areas rather than in

the technology itself.

"Although secure networks such as GCSX provide local authorities with a critical enabling technology, it is down to senior management to make sure their people take personal responsibility for how sensitive public information is handled and shared and that they understand the potential consequences to them, as individuals, if a breach occurs."

In the future, things might look very different. The Cabinet Office has recently announced a range of projects that are in part aimed at improving data security in the public sector, as increasing amounts of public and private information are held online or on local databases. It hopes the G-Cloud will provide a safe environment on the internet for public sector bodies to store data safely, and that the Public Sector Network will become a trusted way to send data across the sector.

In the meantime, the amount of data organisations are required to store has mushroomed over the past decade, and doesn't look likely to stop growing. Coming up with effective policies might be a difficult challenge but it's an area that will need attention if the number of security breaches councils suffer is going to fall.

● **More on the Cabinet Office Security Policy Framework:**
www.cabinetoffice.gov.uk/spf

PREVENTING SECURITY BREACHES

Some of the measures taken by the councils that have suffered breaches:

- Staff dismissed
- Staff training
- Review of procedure
- Forbidden use of discs and pen drives
- Segmented school networks
- Improved security audit, IT security now reporting to Audit Committee

COMMENT

COLIN WISBY
Principal consultant
VEGA Consulting Services Ltd



To deliver efficiencies we need to share data safely

The benefits to the transformational agenda of good security controls are well recognised by local authorities. However, committing to investment in information security, when being asked to deliver ever-increasing efficiency savings, can be a tough ask. But should it be?

With information technology considered key to delivering efficiencies and improvements, ensuring security must be seen as a vital business enabler at board level.

As part of our work advising government on how best to secure data, my colleagues and I have been working alongside the Government Connect programme to complete the provision of the GCSX network. This will prove vital to securing local government data exchanges and the ability to deliver more for less.

However, at the same time as improving capability, the provision of more information means increased security risks. Failure to address these hinders an organisation's ability to deliver efficient services and makes it susceptible to public criticism and litigation.

From 6 April, the Information Commissioner's Office (ICO) has had the power to issue fines of up to £500,000

to organisations in breach of the Data Protection Act. The ICO continues to report on security breaches and it is evident these have had a range of consequences on business operations.

To address these risks, Government Connect has held a series of GCSX Forums across the country. These gave an overview of the Public Sector Network and raised awareness of the Cabinet Office's Security Policy Framework (SPF) and the tools available to assess an organisation's information assurance maturity.

A theme from these forums has been "is this being mandated?" This implies some authorities find it difficult to act and only do so when they have no other choice. This has to be the wrong approach.

Thankfully, as this survey shows, some authorities are being proactive and have already reviewed the SPF and are assessing their information assurance maturity. These are to be commended, as are those that are recognising the issue at board level.

There has never been a greater need to enable secure data sharing to improve public services. With information security high on the political agenda, the decision to invest in best practice security policy has to be self-evident.

COLUMN SPONSORED AND SUPPLIED BY VEGA
WWW.VEGA.CO.UK