

November 2009

Connecting the Public Sector – Executive Summary

- Safeguarding citizen data in an unsafe world



Published by LGITU magazine, with support
from www.UKauthorITy.com, Tomorrow's
Town Hall and Government Connect.

© Informed Publications Ltd, November 2009



Data Security, Frontline Services and Secure Communications

Can local government and other frontline services keep citizen data safe in this new era of collaboration and service transformation?

As the March 2009 deadline for joining up to the government secure extranet, GCSX, loomed, Richard Steel, former president of Socitm and CIO of Newham - and GC Programme Board member - wrote, "We are learning, through Government Connect, that central and local government can work well together. Okay – mistakes have been made, and lessons have been learned, but in less than a year, spectacular progress has been made in joining-up securely and efficiently. Good job too! If ever there was a need for secure, efficient and joined-up government, high profile data losses and the credit crunch conspire to tell us it's now!

"Government Connect lays the foundation for a single pan-government security infrastructure. It can't make sense, and is spectacularly inefficient, for local government to engage separately with each central government department. I'm delighted, therefore, that the Government Connect team aims to work with the Public Service Network programme, and related developments to advance the vision, further enhancing our ability to deliver public services securely and efficiently and demonstrating that Government really can connect!"

Government Connect extended the deadline for many councils to complete their CoCo (code of connection) until the end of September. Over the summer, LGITU magazine began to ask:

- Is there a need to share sensitive citizen data outside the organisation?
- Are councils routinely sharing such data with other local authorities or other parts of the wider public sector?
- And if so, how are councils sharing this data?
- Is the sector implementing the LGA 'best practice' Data Handling Guidelines?
- Would the process of gaining what is essentially a 'certificate' acknowledging high security standards ingrain the importance of data security across the sector?
- Would all councils achieve this high level security assessment by the final deadline?
- Can the public sector therefore meet the dual needs of safeguarding sensitive citizen data whilst sharing information to deliver efficient, improved public services?
- Can connection to a secure pan-public sector communication network bring ongoing benefits?

LGITU magazine, in partnership with its sister online publications, www.UKauthorITy.com and Tomorrow's Town Hall, approached the Government Connect team for support in undertaking this project. Government Connect generously funded the data collection and research activities, ceding editorial control to the LGITU research team.

The project aimed to gather views and opinions from senior frontline officers – from both the technology and departmental user perspective. The research was conducted in, and is reported on, an anonymous basis. However, details of councils participating and the job titles of respondents to the two research tools can be found in Appendices I and II.

This executive summary, published in November 2009, outlines the key findings from the research project.

The full report can be downloaded here: www.ukauthority.com/Connecting

© Informed Publications Ltd, November 2009

All rights reserved. This survey was researched and written as a snapshot of local government and other frontline public services attitudes towards the safeguarding of citizen data within the context of transformation of local service delivery. Whilst every care is taken, the publishers and project partners accept no liability whatsoever for the content or accuracy of this research and the opinions expressed in this report.



Connecting the Public Sector - Executive Summary

In an era of high profile data loss and data leaks, why do local authorities still put sensitive citizen data in the post? Helen Olsen, managing editor of Informed Publications, reviews the findings of LGITU magazine’s survey assessing how sensitive citizen data is shared across frontline services today.

As a citizen it is astonishing to learn from this research that, despite almost two years of media headlines covering the most basic and unbelievable ‘accidental’ data losses, local authorities up and down the country still consign sensitive citizen data to the vagaries of Royal Mail - or worse, to unsecured laptops and removable media that then get left lying about.

From the continuing crop of stories on the news pages of national and specialist press, the Information Commissioner is no less exasperated. A number of councils have had their knuckles rapped in the last couple of months, and a quick look at the excellent Public Sector Forums’ Public Sector Data Breach Log 2009 lists 23 such incidents occurring in UK local government alone in the three months prior to writing this report.

LGITU’s research, conducted over the same time period - late summer 2009 - looked at who was sharing what, and with whom, across frontline services when it came to citizen data. With support from Government Connect, its sister online news services, UKauthorITy.com and Tomorrow’s Town Hall, LGITU magazine conducted two surveys:

- an in-depth questionnaire (103 respondents)
- a quick poll among those not participating in the in-depth survey (105 respondents)

Response	% of organisation type
Police	7.7%
Fire	8.8%
Health	4.8%
Local Authorities (all response)	43.9%
Unique authorities	34.4%

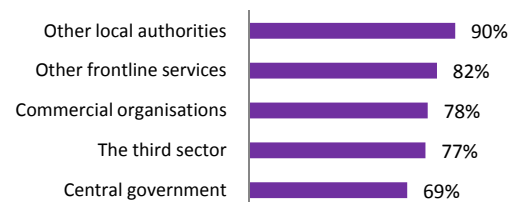
Both surveys had over one hundred respondents from the breadth of local authority types, from across the country, with a number of police, fire and health organisations also participating. The response rate for local government was 34.4% - over one third of all UK authorities. Approximately two thirds of these responses came from departmental users, one quarter from heads of IT and IT seniors, and the remainder from chief executive/councillor/senior corporate officers.

Unsurprisingly, over 98% of respondents dealt with citizen data – those that did not were in GIS, land charges or land & property gazetteer departments. Arguably, whilst their work would revolve around property-based data, communication about this data with the citizen would still necessitate the collection and handling of citizen data. Across both surveys, almost eight in ten (79%) shared sensitive citizen information with other local authorities or other parts of the public sector.

What is the corporate attitude to sharing citizen data?

The LGA published a set of Data Handling Guidelines for Local Government last November. These were developed in partnership with Socitm, and endorsed by Solace and the IDeA, in a bid to stem the flow of data loss from the public sector and foster a culture of data protection.

■ YES - we share citizen data with: (source: indepth survey)



It was surprising therefore to learn that not all councils had an ‘Information Charter’ outlining how citizen data is handled – just 40% said that their council did. Researchers wondered at first whether this could be simply lack of awareness on the front line, but 23% were quite sure that there was no charter in place – in direct contradiction of the Data Handling Guidelines. The remainder, nearly four in ten, were unsure.

Reassuringly, over nine in ten (93%) were sure that all personal information was kept within secure ICT systems – in accordance with the guidelines.

From the detailed survey, however, a disconnect starts to appear between the central/high-level view and that in the technology and user departments. Looking at items from the LGA Data Handling Guidelines, corporate/chief executive respondents all answered either yes or ‘don’t know’ to questions about ICT systems being specified in line with government data security minimum standards; their council having a Corporate Information Risk Policy, and having all the council’s key Information Assets classified and allocated an ‘owner’. None of this subset answered no to these items.

In marked contrast, few of the technology or departmental respondents said ‘yes’ to the above. This group accounted for 38% of the total sample saying either they did not know or that their council definitely did not specify minimum government data standards in ICT systems’ procurement. A total of 45%, again all technology or departmental respondents, said ‘no’ or ‘don’t know’ to their council having a Corporate Information Risk Policy.

Twenty nine percent said that Information Assets were definitely not classified; with a further 42% not knowing whether or not they were. Thirty four percent said that information assets were not allocated owners, with a further 36% not knowing whether they were or not.

In summary, the chief executive group was saying ‘yes’ to these questions; while the majority of the technology and user groups were saying either ‘no’ or ‘don’t know’.

The intentions are evidently there, but the practice is not filtering through.

One further question highlighted this disconnect from the centre: Do councils have a Senior Information Risk Owner (SIRO) owning information risk? Just one chief executive said no. However, two fifths of the technology group and nearly a third of the departments said no. In total, 30% of the sample said that there was no SIRO at their council; with a further 32% unsure.

Worryingly, in light of the unending stream of data loss and data breach stories in the media over the last few years, whilst the majority of corporate/chief executives said that there was a clear incident reporting mechanism in place for such occurrences, 14% of the sample said that there was not, and 27% did not know.

It is disappointing, to say the least, that so few of those working with sensitive citizen data could answer ‘yes’ to this question. More worryingly, just two thirds (66%) said that staff were regularly trained regarding the sensitivity of citizen information and the importance of adhering to the correct procedures for its handling.

The answer, of course, should have been 100% ‘yes’ in both the above instances.

Indeed, not one chief executive respondent said that their council did not have such a policy or training mechanism in place. Which, of course, would be the correct answer: all should have both policy and training.

Results from the quick poll verified this finding: 63.8% answered yes to the same question. But that leaves nearly four in ten either not sure or, worse, definitely sure that their council did not have regular training on how to handle sensitive data.

One said that training was “piecemeal at present. GC is changing this as we are required to actively train all staff accessing IT systems.” Another, very honestly, replied: “Policy exists but formal and recurring training does not.”

These results contrast starkly with the finding that 96% of respondents felt that the legal requirements of the Data Protection Act impacted the way in which they handle citizen data. Nearly eight in ten (79%) felt that the Human Rights Act, and 94% the Freedom of information Act, had an impact on the way their council handled sensitive citizen data.

It is clear that the importance of keeping citizen data safe has permeated throughout local authorities. But the practicalities of ensuring that this be so – for example by implementing the LGA Data Handling Guidelines throughout the authority – are not filtering down to the troops.

Is there truly a need to share sensitive citizen data?

Well, 77.1% of the quick poll said that in order to improve the quality and efficiency of public service delivery, yes, there was: “Immensely so – for place shaping, service take up, increased customer insight, offering of value added services and, most importantly, preventative services,” said one.

Added another: “There is clearly a need, as all headline cases of child abuse could have been prevented if agencies communicated with each other.”

In the long survey we explored the drivers for secure data sharing. Shared services would obviously require secure exchange of information according to 82% of respondents. Mobile and flexible working also required this capability in the minds of 81%. For 67% ‘Tell Us Once’ and for 61% MAPP (Multi-Agency Public Protection Arrangements) required secure exchange.

One senior IT officer noted: “(The) personalisation agenda requires secure data sharing. Partnership activity also, he said, “appears to focus on protocols and high level contact. More detailed work is needed to make the partnerships more effective at a data sharing level.

“It would help if e-GIF were treated seriously – local authorities actively rather than passively ‘encouraged’ to share information, and application suppliers forced to invest in integration and data exchange as a basic part of their packages not as expensive, bespoke add-ons.”

Interestingly, in the long survey, just 13% felt that the new Total Place proposition would require secure sharing, with almost three quarters (73%) not sure. When the quick poll was conducted approximately six weeks later, however, the situation was reversed – perhaps more was by then known about this new approach – with 76.2% saying that, yes, trusted and secure data sharing would be essential in order to deliver ‘Total Place’ public services.

Training for data handling: “Piecemeal at present. GC is changing this as we are required to actively train all staff accessing IT systems.”

Training for data handling: “Policy exists but formal and recurring training does not.”

Need to share? “There is clearly a need, as all headline cases of child abuse could have been prevented if agencies communicated with each other.”

Need to share? “(The) personalisation agenda requires secure data sharing.”

Need to share? “Immensely so – for place shaping, service take up, increased customer insight, offering of value added services and, most importantly, preventative services.”

Total Place: “Unless this data is shared an informed and holistic view cannot be taken on issues such as where services need to be better targeted.”

Information Security: “...is not just about confidentiality. It is also about data quality and availability, which is the real key to cost-effective frontline service provision.”

Stated one respondent: “Total Place looks at how a whole area approach to public services can lead to better services. In order to achieve this it requires data analysis across the whole area. This data will come from a range of service providers on a range of different criteria, ie information on crime and anti-social behaviour.

“Unless this data is shared an informed and holistic view cannot be taken on issues such as where services need to be better targeted. The approach must be evidenced based and cannot be delivered by a single agency or group.

“It needs a consistent and collaborative approach which eliminates duplication and joins up activity.”

It is hard to see how this can be achieved without a secure information sharing platform. GCSX will inevitably play a key role - how else can you uniformly and securely share necessary information or enable secure joint working across the police, NHS, local authority and central government within an area?

The common denominator, the secure government infrastructure, will, by 2012, become the next generation Public Service Network. It is hard to see how the public sector could justify missing the opportunity this presents in tough economic times.

However, coming back to the drivers and the LGA Data Handling Guidelines, it is worth noting that just 58% of respondents said that the guidelines would require secure data sharing. Which, feel the researchers, rather misses the point.

Indeed, whilst the value of information was recognised, researchers detected confusion as to what these guidelines were and how they should be implemented – how information security could be aligned with the business process.

Said one departmental respondent: “Information security is not just about confidentiality. It is also about data quality and availability, which is the real key to cost-effective frontline service provision. Information security also needs to be aligned to the strategy of the organisation and built into its business process.” But, he added, “Please give clear guidance on how to allocate a SIRO.”

So who shares with whom?

Data was currently shared by 78% of the sample with other local authorities, by 74% with the police, 71% with DWP, 64% with the Audit Commission, 59% with HMRC, 56% with HM Courts Service, 56% with health organisations, 51% with schools, 47% with CLG, 42% with DCSF, and 47% the Ministry of Justice.

The organisations’ databases that most would find helpful to have electronic access to in their own office were: National Fraud Initiative (62%), National Blue Badge Register (60%), DVLA (59%), National Pupil Database (54%), Joint Asset Recovery Database (53%), Hospital Leavers & Admissions Database (52%), Persistent Offenders Register (50%), Electronic Patient Care Records (50%). Interestingly, only just under half, 48%, thought that access to ContactPoint would help.

Indeed, the potential for service improvements was not lost on respondents: “If we are to improve health and social care as a whole there will be a need to share data across several organisations.”

One fire authority said that sharing information with PCTs “will help us to identify vulnerable people... and enable us to target them with community safety initiatives to help drive down the incidence of accidental dwelling fire.”

There is a definite opportunity for innovation in the use of data to improve services. Take the DWP’s CIS - finding and fighting fraud is the obvious use, but what about using CIS data to inform a proactive concessionary parking service? It could check the status of invalidity benefit and DLA and simply issue a continuation of a blue badge, rather than making the resident go through the whole application – and proof of eligibility – process again.

And how is this shared?

Whilst it was encouraging to see that, where appropriate, information was being shared, in many cases it was disappointing to see that not all use secure communication routes to share this data.

A frankly astonishing 45.7% in the quick poll shared sensitive citizen data by post/paper or removable storage media.

In the long survey, 44% regularly used paper/post/courier and 22% USB/CD/post/courier combinations to send sensitive citizen data to other local authorities. Almost three in ten (28%) and 12% respectively used these methods when sending data to central government.

In light of the constant haemorrhage of data loss suffered by the public sector in recent years this can be described, at best, as unfortunate.

Service improvement:
“If we are to improve health and social care as a whole there will be a need to share data across several organisations.”

Service improvement:
“(it) will help us to identify vulnerable people... and enable us to target them with community safety initiatives.”

Awareness:
“Government Connect has helped raise some awareness, but many councils (connected and unconnected) remain in an immature IS-capable state.”

Awareness: “There is still a perception among many... that ordinary email is a secure system.”

Awareness: “There are so many agencies involved and with an interest. We need to get together to discuss best practice.”

Cultural change: “There have been too many highly publicised data breaches for the general population to have full confidence in public sector data handling. However, whereas technical solutions can be introduced and improved, the biggest challenge, from my perspective, is the education of data handlers.”

Apart from the risk of loss or theft there is also the unreliability of the post to consider - CRB checks stuck in postal strikes will hold people up from starting jobs. Ongoing industrial action by the Communication Workers Union (CWU) in the second half of 2009 only increases the risk – with reports that much of the post held up in London industrial action late summer may never be delivered. The internet goes down, yes, but not as often as the post these days. In addition, the GCSX has back up and business resilience built in to its contracts. There is no reserve postal service waiting in the wings.

On a more positive note, however, 54% of councils now use the secure government network (GCSX) and 15% a secure point to point connection when sending information to central government. And 41% used the GCSX to share sensitive data with other authorities.

In the quick poll 61.9% said that they used the GCSX to share data. Indeed, from the comments relating to this section it would appear that the programme has gained significant traction in recent months. Many indicated that they would be using the infrastructure more often once everyone was connected at the end of September: “Not yet,” said one, “But we will begin to as we have just had our GCSX connection approved.” Another said that the network was “currently being rolled out throughout this authority”.

The lack of uniform approach across the sector was recognised by one respondent, who suggested that base security levels would need to be mandated to see progress: “Until all councils have mandatory and auditable board-level ownership of information security risk, the situation will remain unsatisfactory. Government Connect has helped raise some awareness, but many councils remain in an immature IS-capable state.”

This view was echoed by a departmental user: “There is still a perception among many people and organisations (not specifically local government) that ordinary email is a secure system.” And there was, said another, a need for a national forum: “There are so many agencies involved and with an interest. We need to get together to discuss best practice.”

However, from the end of September, when all local authorities are required to connect up to the secure government communications infrastructure, there should be no excuse for entrusting sensitive data to the post or courier either on paper or removable storage media.

Indeed, speaking as a citizen, for all citizen data the preferred option should be a secure communication channel. How many parents wait nervously for the day those ‘lost’ child benefit disks turn up in a pub car park?

For local-to-local or local-to-central/other frontline services, the secure routes provided by GCSX and the wider secure government network should be the first option considered. Apart from the security, just think of the time and cost savings. Add in the carbon reduction element and, again, from a citizen point of view, it’s a winner.

However, whilst many respondents had interesting views on the challenges around data security and frontline service delivery, the greatest was identified as “human behaviour (compliance)”. Although this was “partially mitigable by technological advances”.

Data sharing was expected: “Citizens only want to tell us things once. The organisational and departmental divides within the public sector are not understood by the citizen when they are accessing services. However, this does place a very high profile on data integrity, security and methods of data sharing.

“There have been too many highly publicised data breaches for the general population to have full confidence in public sector data handling. However, whereas technical solutions can be introduced and improved the biggest challenge, from my perspective, is the education of data handlers.”

Whilst there is no doubt that understanding of the importance of safeguarding sensitive citizen data has permeated to the highest level, and that the technology infrastructure is now in place, our research finds that the cultural change needed to underpin data security is lagging behind the ‘logical move’ to secure electronic communications.

To fulfil the vision of data security that both the citizen can have faith in and that the organisation can trust to underpin efficient citizen-centric service delivery, the message of just how important citizen data is must be communicated to every public service worker – from top to bottom. Citizen data is not just sensitive to the citizen whose data is lost, it is also one of the public sector’s greatest assets – capable of informing and transforming service delivery. As such it should be safeguarded and nurtured by all those involved in public services.

As this report is published, in November 2009, all UK councils are connected to GCSX.

It will be interesting to see how this new capability to communicate securely between frontline services and across the wider public sector can help improve public service delivery over the coming year. With GCSX in place the barriers to close working between organisations are no longer technical or cost. Culture, as ever, may be the biggest barrier facing joint working teams or shared services initiatives as the sector faces perhaps its most difficult times.

The perfect storm of spiralling demand for services in the face of inevitable budget cuts will prove one of frontline services greatest challenges. Will the sector look to existing infrastructure to make the most of available resources?

To download the full report visit: www.ukauthority.com/Connecting