Roundtable: A secret gathering

As the government deals with more digital information and online services, its traditional ways of managing data security are looking outdated. Mark Smulian reports on a Civil Service World round table debating the issues.

When the Serious and Organised Crime Agency had to take its website offline in June following a concerted 'distributed denial of service' attack by now-disbanded hacker group LulzSec, it was a reminder of the risks to public organisations that venture onto the web. Indeed, even storing information in a digital format carries its dangers: many government bodies have lost or accidentally released such data – and whenever electronic info held by the government turns up in public, an outcry ensues about lax security.

In the old days, sensitive data would be stamped 'secret' and hidden away in a locked filing cabinet. But these days the need to foster greater transparency, move public services online, and produce savings by using new technologies makes that impossible. Last week a CSW round table discussion, sponsored by data security specialist Sophos, debated how to keep information secure in a fast-evolving data-management landscape – and concluded that the main challenges are not technological, but revolve around culture, education, a lack of risk-management skills, and an absence of peer knowledge networks.

Diane Wailing, head of reporting and compliance in the Government Security Secretariat at the Cabinet Office, pointed out early in the discussion that cultural changes have already led to changed attitudes towards security – posing new challenges for those responsible for data protection. "You can put in place all the technological barriers you like, but if people have a mind to they will share information they should not," she said. "More often than not, they are just trying to be helpful."

When the private becomes public

The problem, participants agreed, has two key facets: technological changes are fast increasing the number of people who can access and move data; and common conceptions of what should properly be made public are breaking down. On the latter point, Paul Dodgson – the head of information assurance at the Driving Standards Agency – pointed out that the onward march of social media is weakening the common understanding of what information is considered 'private'. He gave as an example his 14-year-old daughter who, when admonished about putting too much personal detail on Facebook, replied that her name, address and date of birth were not secret because they helped people to get to know her.

People with such attitudes to privacy are – or soon will be – entering the civil service, and Wailing wondered: "Where does the line come between what you do at home and at work? Those boundaries don't exist any more, and we need to get to the culture where we can say: 'This is appropriate for the office, but not appropriate for sharing on your home system'."

Jennifer Rigby, chief information officer at the Department for Energy and Climate Change, agreed: "We have people coming to work in government who do not understand there are different ways to behave in an organisation from the way you behave outside with your own information," she said. "It is a huge issue across the generations to educate people about what it means to own your data; that it is a valuable resource and you should care about what happens to it."

Setting the privacy level

To be fair, the lack of clarity around information's sensitivity is not helped by the UK's patchwork of ageing classification systems. James Lyne, senior technologist at Sophos, suggested that the existing government system – which dates from the Cold War – needs to be updated for an e-enabled world. The system "becomes increasingly untenable with changes of attitudes to accessing

information," he said. "But what replaces this Draconian classification scheme we are used to? And how do we help people avoid losing data and move to a risk-based model?"

Indeed, Dodgson complained that there is no common definition across government of what 'confidential' means, leading to leaks through misunderstandings. "We need something useable across government. You've got the NHS saying things are 'in confidence', when in government 'confidential' means something else and 'business confidential' is something else again," he said. "You can start with something of impact level four that another organisation sees as impact level two, and it is the same information."

Faced with such uncertainty, many civil servants are tempted to play safe and put material into highly restricted categories, said Lyne – but this approach will thwart the transparency agenda. Rigby also said that people tend to classify a whole data set according to the most sensitive data in any of the documents it contains – but that means that any data set with even a few such documents will unnecessarily "end up having to go to the highest level".

What's more, contributors pointed out, the current set of systems are ill-equipped to handle the complexities around modern methods of communication. Ben Aung, information security architect at the National Archives, said that until recently the meaning of 'restricted' was obvious – but "suppose now I am in an e-mail conversation chain, and as individual e-mails they are nothing, but in their connections they give a picture. _"I do not think the protective marking scheme is designed to deal with that," he said. "We do not have a fit-for-purpose tool."

Talking of tools, Lyne pointed out that rapid technological change and fast-moving communications markets are pushing a constant stream of new devices and applications into people's hands. This is "a hugely disruptive trend in security handling, but also an opportunity to reduce cost", he pointed out. "We cannot say 'no', but it is a huge challenge to say 'yes'."

Later, he raised the prospect that classifications could become advisory rather than mandatory, forcing staff to think about their own responsibilities and creating a system flexible enough to cope with evolving technologies. “It takes quite a lot of maturity to use this classification as advisory, and defer a lot of responsibility to end users. Whilst some data will always need to be protected with the utmost secrecy, much of it would be better handled by letting users behave sensibly,” he said. “I think we are at the point where we need to do that unless we are going to say we reject iPhones, iPads, Androids and other new technology, and will not increase transparency”.

When private + private = public

The proliferation of new digital devices sits alongside other dynamics that are increasing the ways in which data can leak out. Because online public services depend on allowing service users to access their own data via the internet, the number of people with access to some government data is bound to increase. Meanwhile, the capacity and portability of data storage equipment continues to develop rapidly.

Peter Topping, programme director at the Department for the Environment, Food and Rural Affairs, highlighted another problem: “People are much more savvy about how to get round things, so you will get an inspector out in the field who finds a way of keeping all his data somewhere that he thinks is safe but isn’t – whereas 10-15 years ago he would not have known how to do it, or the [data] wouldn’t have been there. I think that is where we will get the next breach.”

Adding another risk to the tally, Dodgson pointed out that even anonymised data sets can yield personal information when combined with other similar data. Some comments by people associated with Lulzsec, he said, had threatened to release anonymised data obtained from public organisations – and that “could result in it being exposed as non-anonymised by the aggregation of two data sets”.

Wailing said this can be a problem even when information is released legally,

since “different departments will release different data sets which on their own are reasonably acceptable, but when you start joining them up you can make inferences that are not actually true but which suit somebody’s agenda – so we need to look at what we are releasing across the whole piece, rather than from a silo”.

Judging the risk

At the root of many of the government’s problems with handling data, some participants suggested, lies a lack of skills in intelligently appraising the risk involved in particular activities. Wailing noted that when specifying security systems, civil servants “assume you have to go for the gold-plated security versions” – but added that as budget cuts bite, these security provisions are often targeted for savings. “We are missing an underlying skill, which is risk management,” she said. “Actually, you need to look at what you’ve got and do the risk calculations and say: ‘Maybe we don’t want that to get out, but it’s not as important as this other stuff that we really do want to protect’.”

Parts of government find risk management difficult, she said, because if things go wrong, those involved “take the flak” for allowing an element of risks. “We don’t have a culture that says: ‘You made a decision. It didn’t work out. Let’s move forward and learn the lessons,” Wailing added.

Linda Cooke, who works in ethics and compliance governance at HM Revenue and Customs, commented that “risk management is seen as something senior management do; but every time you look at a document and decide classification, it’s a kind of risk management and it should be integral to everything we do”.

People should take more responsibility for risk-managing their own work, she argued – and Simon Lovett, head of knowledge and information management at the National Archives, agreed. “It comes back to the language you use to talk about risk,” he said. “If people are thinking about information being an asset or a

liability, then they can think about what they creating."

Secret communications

One thing that might make civil servants more comfortable with risk management is the ability to ask their peers to discuss problems, and to track down solutions already arrived at elsewhere in government, in an atmosphere where people are open about their mistakes and what they've learned from them. But such networks are rare. Aung noted that "groups do exist – and where they work, they work really well – but if anything they are being scaled back."

Nonetheless, Aung drew encouragement from the response to several recent high-profile cyber attacks. These, he said, have engendered "a sort of amnesty where people now think: 'Some bigger players than me have been done over, so if I come out and admit that I had data loss they will be a bit more accepting of my failures'."

Ollie Hart, Sophos's head of public sector for the UK and Ireland, pointed out that the round table had revealed a common desire for more such forums. "The desire to share experience has come out from almost every point in this discussion," he said. "There needs to be a platform where cyber-security and information assurance people can get together."

Dodgson agreed: such networks would be useful because "if something new comes along, I want to know: has somebody already done something better that will save me time and money?" It must be clear to those involved in combating data loss or theft, he argued, that "they have a responsibility to share, because without that they will be reticent in sharing, assistance and collaboration".

Perhaps, suggested Aung, there should be a network of different groups to allow professions to learn from each other – a point echoed by Angela Duncan, information assurance compliance and standards manager at the Home Office, who argued that many of the relevant professions need to build much closer

links. “I don’t think that is the message that is getting across at the moment,” she said.

A federation of linked networks would be the best arrangement, said Wailing, calling for something “a bit like the social networking model – but joining them up to ensure that they talk to each other needs to be managed: it needs a big spider at the centre of the web”. Any volunteers?

Concluding comments

Ben Aung, information security architect, National Archives: “We need some effective mechanism for knowledge sharing at all levels where people feel they can influence each other, share best practice, and feel comfortable and confident enough about their failings to learn from them”

Linda Cooke, ethics and compliance governance, HM Revenue and Customs: “I’m from the department that lost the disks, and there has been a huge panic across government – but sadly [since then] levels of awareness have tailed off.”

Paul Dodgson, head of information assurance, Driving Standards Agency: “We have got to ensure proportionate information assurance [IA] and connect with people outside IA in a coherent and consistent way”

Angela Duncan, information assurance compliance and standards manager, Home Office: “Cyber-security and IA can’t be separate. They have got to be together”

Ollie Hart, head of public sector, UK and Ireland, Sophos: “Don’t have that fear of asking questions. Don’t be afraid to go and ask the private sector to give advice.”

Simon Lovett, head of knowledge and information management, National Archives: “What we should take away is the need to come up with simpler, stronger, more unified language around what these issues are, to reach a wider audience”

James Lyne, director of technology strategy, Sophos: "We are probably at the most significant point of transition since we all moved from the mainframe. Everything is going to change faster than ever before, and it's only going to get worse, so we must make sure we have the forums and support to exchange ideas. If we cannot learn from each other and share experiences, then all this technology is going to run away far faster than we can ever hope to catch up"

Jennifer Rigby, chief information officer, Department for Energy and Climate Change: "It is not just information security, but knowledge and information-management professionals and others across the piece that we will need for our networks"

Peter Topping, programme director, Department for the Environment, Food and Rural Affairs: "How do you create the burning platform that gets [cabinet secretary] Gus O'Donnell, or whoever, to realise something has to be done?"

Diane Wailing, reporting and compliance, Government Security Secretariat, Cabinet Office: "Nothing stands on its own. We are all interconnected and need to join the dots up; we need someone to bring the different parts together"

Chair: Suzannah Brecknell, deputy editor, Civil Service World