alarm
THE PUBLIC RISK MANAGEMENT ASSOCIATION

ZURICH MUNICIPAL

Information governance and technology

New technology offers significant benefits for local authorities, their employees, partners and suppliers. It can help reduce costs, create flexible working options and fulfil today's communications, accessibility and transaction requirements. For example, communicating online can be a valuable means of engaging younger people.

However, there is a downside. Protection of sensitive personal information is crucial, while today's technology can extend risk exposures far beyond those traditionally associated with IT.

Local authorities can hold a great deal of sensitive information about the individuals within their communities, ranging from online payment details and welfare benefits to health and social issues. Protection is key to avoid regulatory and reputational repercussions.

Common misconceptions

It is a common misconception that cyber attacks, committed maliciously or with criminal intent, are the most serious danger. For this reason, data protection may mainly focus on IT solutions such as firewalls, robust passwords and data encryption. Clearly it is important to have all of these in place but in fact most breaches for local authorities occur because individuals possessing data fail to understand the possible ramifications of how and where they use and transfer it – and to whom.

As such, data is no longer restricted to office computers. Employees use many devices which enable mobile working, for example, smart phones, tablets and laptops. Having third party sensitive information on such devices – or the ability to easily access it from them – widens the likelihood of a data breach.

Managing data

The pressure of recent budget cuts and the need to provide "more for less" has also increased this likelihood. Local authorities have adopted a number of ways of managing data , including outsourcing, partnering and sharing services. One result of this is that information is being shared with more organisations and they are having to rely upon these to implement appropriate IT risk management and data protection.

What the research tells us

Research conducted for Zurich Municipal by Ipsos Mori last year shows that local authorities are very confident about their ability to manage data protection. Almost all (99%) of the local authorities' chief executives and directors interviewed were confident that they have the capability to protect sensitive data.

However, the latest analysis from ICO, published on 11 March 2015, shows that local authority data breaches ranked second in incidents by sector in the previous year. (The health sector being first, and the education sector third.) This performance suggests a significant gap between perceptions and reality.

The regulator's role

The Information Commissioner's Office (ICO), the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It provides guidance for organisations and those involved directly in handling data, and has the authority to issue fines of up to £500,000 for serious breaches of the Data Protection Act and Privacy and Electronic Communications Regulations.

“We believe the traditional controls we have in place to protect us from cyber risk (firewalls, passwords, encryption of data etc) are sound, but the greatest risk now comes from human error, such as sending sensitive documents to the wrong person or losing files in transit. One of the ways we are combatting this is with e-learning which provides staff with the information they need to manage data and information properly and has the added advantage that we can track when people have accessed and completed the training”

Local government risk manager’s comments

Risk consequences

Failure to protect data can result in:

- Imposition of penalties by ICO including potentially hefty fines
- Information getting into the “wrong hands” potentially resulting in extortion, theft or malicious attacks against the affected individuals
- Liability for damages
- Threats to service delivery and other local authority activities
- Significant loss of reputation, with disaffection of employees, partners and the local community.

Zurich Municipal’s view

Although our research last year showed that local authorities were confident about their ability to manage data protection, we believe that this view is based on the robustness of their technology. However, analysis of recent ICO fines against local authorities shows that very few (if any) are the result of hacking or other on-line theft. Human error or failure to take care of sensitive information removed for home-working are the main causes in recent years.

For example, social care workers’ role in the community necessitates the use of mobile devices. Using outsourced services can compound problems as it is more difficult to enforce and monitor secure working when dealing with external organisations.

Data protection is largely a behavioural risk so it cannot be left purely within the remit of the IT manager. All employees that handle data need to know how to manage it safely.

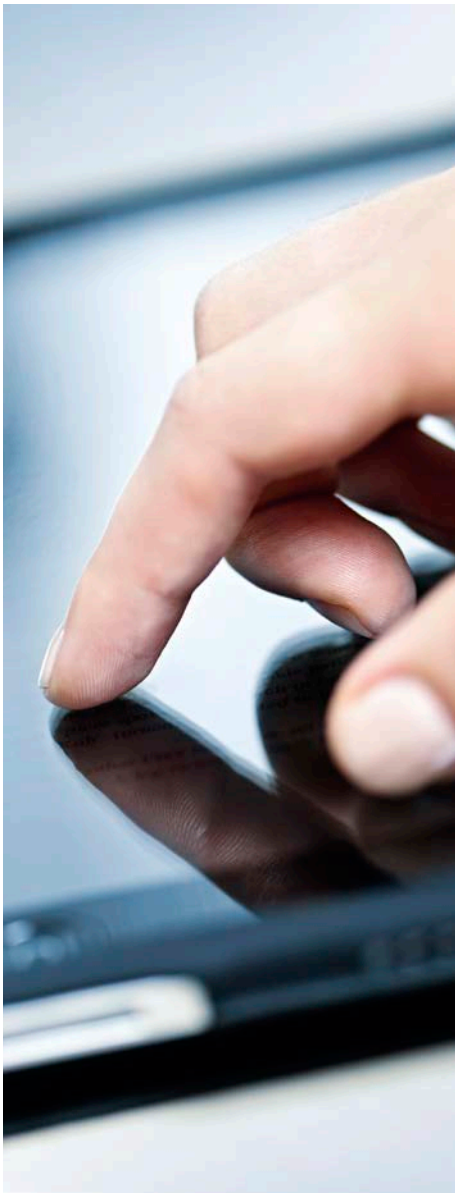
How safe is your data? Questions to ask yourself

- Do you understand and manage the complete risk cycle, starting from when data is created through to its eventual archiving or disposal?
  - Why is the data being created?
  - How is it being disseminated?
  - Who are you sharing the data with – and how is it being used?
  - Where and how is it being stored?
  - Do your storage providers have robust protection policies in place and how do you monitor these?
  - Do you have up-to-date retention and archiving policies?
  - Have you made adequate provision for disposal and, if you are using an external disposal company, are they carrying out your instructions appropriately?
- How good are the security systems of those with whom you share data, such as suppliers and partners?
- Have you evaluated the possible costs associated with technology risks – in reputational as well as financial terms?

Potential strategies for data management

Local authorities appreciate and utilise the benefits of technology but also need to take account of the potential risks – and manage them. Strategies include:

- Having an effective system for classifying data in terms of sensitivity and confidentiality
- Ensuring that employees whose work involves access to sensitive data understand the need for protection. For example, data should only be transferred if essential and to a partner who is equally responsible regarding protection
- Implementing prevention and detection controls so that potential data breaches can be identified and dealt with quickly
- Understanding the true costs of mitigation which, in a serious case of data breach, can far exceed the costs associated with other consequences such as fines and reputational damage
- Being aware of the effects of changes such as new responsibilities for public health which involve patient-identifiable data
- Providing appropriate training for individuals handling sensitive data.



Contact us

If you have any questions or if you would like to talk to one of our team please contact us at **info@zurichmunicipal.com**
You can also read interesting newsworthy articles around key topics at **newsandviews.zurich.co.uk.**

Visit our website at **zurichmunicipal.co.uk**

@ZurichMunicipal

Further reading

ICO Data breach trends
https://ico.org.uk/action-weve-taken/data-breach-trends/

Information governance in relation to local authorities and their new roles in health, Local Public Health Intelligence
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/212965/Public-health-intelligence-information-governance.pdf

Guidance for local authorities on the use of social security data, Department for Work and Pensions,
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307156/data-sharing-guide-april-14.pdf

PP401890001