Chorley Borough Council:
Cyber Risk and Information Governance Review

Final Report 05/06/2015

Victoria Gibson, Strategic Risk Consultant
David Penter, Strategic Risk Consultant

Zurich Management Services Limited
Registered in England: No 2741053
Registered Office
The Zurich Centre, 3000 Parkway
Whiteley, Fareham
Hampshire, PO15 7JZ

1	**Introduction and Methodology**
1.1	Cyber and information risk is an area of increasing concern for any organisation which uses IT systems and technology to handle personal, sensitive or confidential data. More complex ways of managing a variety of information and data, via different media, and across a number of partners, incurs greater potential for risk. The Council's ability to secure its information, people and reputation is essential. Chorley Borough Council (CBC) commissioned Zurich Municipal to conduct a cyber and information risk management exercise, to highlight any potential areas of vulnerability and assess the current risk exposure of the Council. Although this is not an audit process it will aim to identify current good practice and help the organisation to improve. This process involved a desktop review of existing documentation and processes, and interviews with senior managers and key people across the council. This report is an outline of key findings from the review and the interviews, with accompanying management actions, which should be viewed as recommendations only. The recommendations from the report have subsequently been discussed by the Risk Manager and the Head of Customer & ICT Services and the actions agreed for implementation are contained in the Management Action Plan attached to the report.
1.2	The overall aims of this exercise were to identify: • Levels of understanding of information management across the Council • Existing good practice • The understanding of roles and responsibilities, e.g. Senior Information Risk Owner • Any areas of concern or potential for improvement • What cyber risk and information governance mean for the council and how to address them
1.3	A desktop review of CBC's policies and procedures and other relevant documentation was carried out, against acknowledged best practice and standards e.g: • The information security standard ISO 27001 • The Freedom of Information Act 2000 • The Data Protection Act 1998 • Computer Misuse Act 1990 • Local Government (Access to information) Act 1985
1.4	A series of confidential one-to-one interviews was conducted, covering several lines of enquiry, including:

	• Context of job role and information governance responsibilities • Knowledge of corporate and regulatory operating environments • Policies and procedures • Incident management • Third party vendors • Social media • The cloud • Mobile devices
1.5	The following people were interviewed (in chronological order): Helen Sutton, Customer Services Manager (Direct Services) Chris Moister, Head of Governance Camilla Oakes-Schofield, Head of HR and Organisational Development Alison Wilding, Customer Services Manager Andrew Daniels, Communications Manager Cath Burns, Head of Economic Development Paul Heyworth, Business Advisor Zoe Whiteside, Head of Housing Gary Hall, Chief Executive Simon Clark, Head of Health, Environment and Neighbourhoods Rebecca Huddleston, Head of Policy & Communications Jamie Dixon, Head of Street Scene and Leisure Contracts Debbie Wilson, Digital Information Manager Adrian Dixon, Senior Technical Engineer Susan Guinness, Head of Shared Financial Services Jamie Carson, Director of Public Protection, Street Scene and Community Asim Khan, Head of Customer and ICT Services Lesley-Ann Fenton, Director of Customer and Advice Services These interviews were intended to encourage open discussion around the organisation's existing information risk management approach, framework and processes and to identify strengths and areas for improvement. Zurich would like to thank all the participants for their engagement and input.
1.6	The scope of this exercise does not extend to a review of IT systems and networking security
1.7	This report is divided into the following sections for ease of reference: • Compliance and Best Practice • Policies and Procedures • Training and Awareness • Social Media • Mobile Devices

<table>
<tr><td></td><td>

- Third Parties
- The Cloud
- Incident Management

</td></tr>
<tr><td>1.8</td><td>

This report presents overall findings and recommendations for management actions arising from Zurich Municipal's observations and the views of the participants. Objective risk ratings are allocated to each section:

<table>
<tr><td></td><td>Perceived to be an area of high potential risk and further management action required</td></tr>
<tr><td></td><td>Perceived to be an area of low or medium potential risk; further actions may be considered</td></tr>
<tr><td></td><td>Perceived to be an area of minimal risk; no immediate actions required</td></tr>
</table>

</td></tr>
</table>

2	**Executive Summary**	
2.1	Over recent years Chorley Borough Council has made a significant investment in mobile technology to bring about improvements in data quality and security. The Council now works with very little paper which reduces opportunities for information leakage through negligence. In the modern world though, there are increased threats from cyber-attacks which would have the ability to disrupt normal activities. The Council has however achieved PSN compliance and this has recently been reviewed and awarded for another year. As such, management has a reasonable level of confidence in their ability to withstand an attack and protect the information assets of the council.	
2.2	At the core of information governance is the Information Security Management Framework which is currently being refreshed and will consolidate a number of separate policies for ease of access. Gaps in the existing framework such as information classification and social media use are being addressed in the updated version. The launch of the new framework will be supported by a communications programme but longer term governance and communication arrangements to maintain focus and understanding in this area need to be formalised.	
2.3	The framework will be underpinned by a sharepoint repository known as Myshare which, it is intended, will make all Council information available across different service areas. Further work is required prior to implementation to ensure that risks of data sharing are properly understood and controlled. This could form part of a more formal consideration of information risks across all service areas.	
2.4	The digitisation of the majority of paper records means that there needs to be additional focus on recovery in the event of system downtime. A review of existing business continuity plans would be beneficial to ensure that they are aligned with system recovery timescales.	
2.5	“Cyber-risk” as a term is not widely used within the Council; it generally seems to refer to technical issues such as hacking or malware. Governance is acknowledged to be important and the governance of data and information (integrity, relevance, accessibility etc.) is widely understood.	
	Overall Risk Rating:	

3	**Compliance and Best Practice**	
3.1	The Council has achieved PSN compliance, which drives many of the policies and working procedures relating to information and IT. PSN compliance has recently been re-assessed and confirmed.	
3.2	There is generally good understanding of the regulatory environment, for example the Data Protection Act, Freedom of Information Act etc. Limited instances of data loss have occurred in recent years which have been brought to the attention of the Information Commissioner's office. No fines have been levied.	
3.3	An Information Security Management Forum existed previously, which has evolved into the Information Security Council. Work is ongoing to update and re-launch the Information Security Policy and, once this is completed, the Information Security Council will also be re-launched with clear terms of reference.	
3.4	A key focus of the IT strategy has been to remove a lot of paper from the office due to the perceived benefits from both a cost and risk perspective. This has led to digitisation of many records. Retention procedures are outlined within the Information Security Framework, with regard to electronic and paper information, which employees are instructed to refer and follow for their own service areas; however, understanding and interpretation appears inconsistent across the council. Record retention schedules did not appear to exist for individual service areas.	
3.5	A new Senior Information Risk Officer (SIRO) has recently been appointed and is currently building her knowledge and understanding of the requirements of the role and the expectations placed on her.	
	Management Action 1 **Once the Information Security Policy is re-launched, re-invigorate the Information Security Council and agree terms of reference that consider the full range of information management activities and requirements.**	
	Management Action 2 **Refresh corporate guidance on records management and ensure that this is interpreted and applied appropriately in individual service areas. Oversight could be provided by the Information Security Council.**	

4	**Policies and Procedures**	
4.1	At the core of the policy and procedural framework is the Information Security Framework which will shortly be re-launched. This is a lengthy document which creates a challenge over its accessibility to employees. The new version will consist of a core framework with several appendices covering more specific policy areas such as mobile working, information classification, social media, etc. which represent gaps in the current framework and will improve ease of reference and accessibility.	
4.2	Accessibility of information is being driven by creation of a sharepoint site (Myshare) with the intention that all council information is accessible to employees in different service areas. There is some divergence of views as to what information should be accessible to all which needs to be resolved prior to launch.	
4.3	Information is also held on a personal drive (P: drive). The intention is to review what is held here and reduce storage limits to force use of Myshare.	
4.4	The reduction in paper records means that there is less risk of confidential information being left unattended. There is no corporate clear desk policy in place, although various service managers apply one to their own area. That said, a periodic reminder of the value of clear desks would be helpful, as it was cited as a challenge in certain service areas.	
4.5	Building security appears satisfactory with access controlled by security passes and CCTV images available in reception areas. Security passes were not always visible but the expectation is that any strangers who had tailgated into offices would be quickly challenged. Interview rooms are available for confidential discussions with customers.	
4.6	All printing is securely done to PIN and limited printers are available within the offices to discourage unnecessary printing. Confidential waste is placed into lockable bins and shredded off-site by a third party contractor.	
4.7	Passwords have to be changed regularly and changes have been forced where they are not considered sufficiently robust. Some frustration was expressed at the number of different passwords required for different systems.	
4.8	Heads of Service are required to provide an annual governance statement which includes a section on Information Management: Internet and Email Acceptable Use Policy, Data Protection Act and Retention Guidelines.	
	Management Action 3 **Ensure proper consultation with all service areas about access to information. Document the policy decision and implement in Myshare.**	
	Management Action 4 **As part of the team brief process, remind employees about the value of a clear desk approach and ensure that managers reinforce any requirements.**	

5	**Training and Awareness**	
5.1	The induction process for officers and members includes a requirement to sign a confirmation of understanding of the Information Security Framework. Daily sign on to systems also requires confirmation of compliance although this is more of an unconscious sign-on. Based on our discussions, the leavers' process for removing access appears to work satisfactorily.	
5.2	Most service areas were able to articulate the information risks they faced but there is no aggregated risk on the council's strategic risk register or at an individual service level.	
5.3	Several service areas referred to the information champion role but were not clear on the specific responsibilities of the individuals. Previously, this was felt to be a useful way of getting updates and training. The role still exists and is now used primarily as a conduit for freedom of information requests. An opportunity exists to clarify the role and the skills and capabilities required of it as part of the Information Security Policy refresh.	
5.4	The launch of the Information Security Framework will be supported by a communications process, possibly involving articles in team brief and a sign off process to confirm understanding. Given the detail contained within the framework consideration should be given to making the document more accessible to the user, possibly through bite-size refresher training. This would also help to address reasons behind decisions taken within IT, for example the reduction in mailbox sizes.	
5.5	Issues relating to information management are raised with Members as required but there is no standing agenda item. Members have faced many of the same challenges as officers as part of the cultural change associated with moving to less paper with all meeting papers now sent via iPad.	
	Management Action 5 **Consider the skills, capabilities and expectations of the Information Champion role and re-invigorate as part of the re-launch of the Information Security Framework.**	
	Management Action 6 **Consider a more formalised assessment of service level information management risks and determine whether they represent an aggregated risk for the council as a whole.**	

6	**Social Media**	
6.1	Use of social media appears well controlled and is used by the council to encourage feedback on specific activities. The social media channels used are Facebook and Twitter and these are primarily controlled from the Communications team. Some service areas have the ability to post items to social media but tend to do so sparingly. Others expressed a desire for more liberal use of social media but there is limited appetite for this from the Communications team at the moment.	
6.2	An external communications protocol is in place and sets out acceptable practices. For example, re-tweeting Member tweets might be viewed as unacceptable if it shows bias towards individual political parties. The Communications team will monitor and delete posts if necessary.	
6.3	Members' personal Facebook and Twitter accounts are not controlled corporately. They are monitored to ensure that they don't create unrealistic expectations or demands on council services	

7	**Mobile Devices**	
7.1	The council has invested significantly in mobile technology with all Heads of Service and some senior managers being issued with iPads. The devices offer access to email services and other corporate systems. In the event of loss or theft any data held on the iPad could be wiped remotely and, as further authentication is required to access corporate systems, the data held in those applications is expected to be secure.	
7.2	Council laptops do not support the use of removable media such as memory sticks. In addition email traffic is monitored to ensure that information is not being sent externally to private email accounts. An example was cited of someone being dismissed for doing this. Should confidential information need to be sent outside the council the information can be encrypted by the IT Service.	
7.3	Some neighbourhood officers are provided with iPhones so that jobs can be issued directly to them. This also assists with data quality as it puts collection at the source rather than relying on paper records being returned to the office.	
7.4	Remote working is possible subject to the provision of an access key from IT. There is no access to webmail.	

8	**Third Parties**	
8.1	Standard contract terms exist in relation to information held by third parties. It is not clear how these contract terms are overseen however or how suppliers provide assurance that data is held securely.	
8.2	Payroll services are provided by Blackpool Council and they also provide the Vision HR system which contains personal data for all employees. We understand that Blackpool and all other suppliers are PSN compliant.	
8.3	Data-sharing protocols are being revised and this is likely to become a consideration of the Information Security Council. The Council overall is likely to make risk-based decisions on data-sharing, on a case by case basis, in order to benefit the community.	
8.4	Data-sharing arrangements are in place with the Department for Work and Pensions (DWP) and JobCentrePlus, to help to reach the most vulnerable communities. These agreements took a long time to get into place because of DPA restrictions and interpretation.	
	Management Action 7 **Consider an approach to assuring the security of data held by third parties which is commensurate with the associated risks.**	
	Management Action 8 **Ensure data-sharing protocols are in place, communicated and understood, to ensure that decisions can be justified.**	

9	**The Cloud**	
9.1	Current use of cloud services within the Council is limited to a small number of applications. Cost and security considerations will be used to determine future cloud services.	
9.2	The data held on the housing web-based system includes personal information and case notes. Survey monkey is also used by certain areas and, again, personal data may be held. There are no specific concerns held by IT with these uses.	
9.3	In order to enhance the resilience of IT services moving forward it is likely that the use of cloud will become more prevalent. Any such developments should be supported by a clear strategy which assesses the risks and the operational requirements associated with assuring the security of information held in the cloud.	

10	**Incident Management**	
10.1	Incidents have had to be investigated on an infrequent basis so the level of knowledge of the process is limited. Prior experience suggests that processes are sufficient and that appropriate actions will result from the investigation.	
10.2	System logs are maintained to support the incident management process and identify which users have taken specific actions.	
10.3	Increased digitisation of records has presented changed business continuity risks which are either not necessarily understood or reflected in current plans. These should be updated and aligned with system recovery times.	
10.4	A disaster recovery site is held at Lancashire County Council offices in Preston.	
	Management Action 9 **Review business continuity plans to ensure that they reflect the changes in work methods and are aligned with system recovery times.**	

Management Actions (Recommendations) Summary

No	Action	Who	Comments	Complete
1	Once the Information Security Policy is re-launched, re-invigorate the Information Security Council and agree terms of reference that consider the full range of information management activities and requirements.	Asim Khan	• The Information Security Policy will be Presented to Cabinet in June 2015 • The Terms of Reference for the Information Security Council will be comprehensively reviewed and revised. • The Information Security Council will be re-established and its role and activity promoted across the Council to raise the profile and awareness.	All action to be complete by January 2016
2	Refresh corporate guidance on records management and ensure that this is interpreted and applied appropriately in individual service areas. Oversight could be provided by the Information Security Council.	Asim Khan	• Corporate guidance on records management will be revised and re-launched • A corporate record retention template will be developed • Each service will develop and implement a record retention schedule appropriate to its own requirements • The Head of Customer and ICT Services will meet with each Service Head to clarify the application of the guidance and assist with the development of the Service record retention schedule	All action to be complete by March 2016
3	Ensure proper consultation with all service areas about access to information. Document the policy decision and implement in Myshare.	Asim Khan	This issue is the subject of an agreed strategy adopted by Cabinet and is also dependent on migration to SharePoint 2013 within 18 -24 months however in the meantime: • The Head of Customer and ICT Services will raise the matter at Information Exchange for discussion in order to quantify areas of concern. • Further consideration will be given to any substantive issues in order to resolve concerns and suitable adjustments will be considered for	All action to be complete by January 2016

			incorporation to the Myshare approach as necessary	
4	As part of the team brief process, remind employees about the value of a clear desk approach and ensure that managers reinforce any requirements.	Asim Khan	• The Head of Customer and ICT Services will arrange for a suitable Item to be included on the team brief to accompany the roll out of Information Security Framework awareness.	Action to be complete by September 2015
5	Consider the skills, capabilities and expectations of the Information Champion role and re-invigorate as part of the re-launch of the Information Security Framework.	Asim Khan	Not agreed – It has been decided to reduce reliance on the Information Champion role for the dissemination of systems development information as it is increasingly less compatible with the Digital Agenda. The role will remain in place as the conduit for FOI/EPA/DSA requests.	N/A
6	Consider a more formalised assessment of service level information management risks and determine whether they represent an aggregated risk for the council as a whole.	Andy Armstrong	• The Risk Manager will arrange for a formalised assessment of service level information management risks to be completed. • The outcomes will assessed for inclusion in the Strategic Risk Register or if this is not warranted passed to the Head of Customer and ICT Services as Customer Consultation data for consideration of appropriate action.	All action to be complete by January 2016
7	Consider an approach to assuring the security of data held by third parties which is commensurate with the associated risks.	Asim Khan	• The Risk Manger will seek further advice from Zurich regarding the development of a suitable approach. • The Information Security Council will then develop a procedure and checklist to enable the data risk to be assessed as high, medium or low and advise on the appropriate assurance action to be taken. • The Head of Customer and ICT Services will liaise with Procurement and Corporate Policy to ensure the procedure is embedded and applied within procurement guidance and the Partnership Framework.	All action to be complete by March 2016
8	Ensure data-sharing protocols are in place, communicated and understood, to ensure that decisions can be justified.	Asim Khan	• When the revised Information Security Policy is launched particular attention will be drawn to the application of Appendix M guidance on Data Sharing and use of the Data Sharing Agreement.	September 2015

9	Review business continuity plans to ensure that they reflect the changes in work methods and are aligned with system recovery times.	Andy Armstrong	ICT Services are currently finalising a revised ICT Service BCP Recovery Plan and as soon as this is complete the Risk Manager will complete the alignment of arrangements within the overall BCP suite of plans.	All action to be complete by January 2016