PERTH AND KINROSS COUNCIL

Strategic Policy and Resources Committee

10 February 2016

Cyber Security

Head of Legal and Governance Services

PURPOSE OF REPORT

This report provides an overview of Cyber Security in the Council and provides assurance as to current risks and threats.

1. EXECUTIVE SUMMARY

1.1 More and more of the Council's business and information is transacted and managed digitally. This information is a key business asset which needs to be protected. This report provides a description of the current arrangements in place within the organisation to protect that information (our "cyber security"). It details the relevant compliance frameworks which the organisation is subject to and gives an analysis of the security measures in place in order to counteract threats and mitigate the risks to provide the Council with assurance as to the integrity of our systems and processes.

By way of context analysis, in November 2015 the following threats were identified:-

- 7,190 emails containing viruses
- 206,311 spam emails
- 1,066,909 malicious connection attempts
- 774 viruses and malware on the network

These were all successfully blocked and there was no reported compromise of Council systems.

1.2 As well as the continuous monitoring of the Council's cyber security by the Information Security Team and IT Division, the arrangements for the security of our digital information is also subject to external reviews and assessments:-

- An annual IT Health Check (comprising both internal and external vulnerability tests) must be undertaken and satisfied to ensure continuing compliance with Public Service Network (PSN) requirements.
- Quarterly network tests are carried out to ensure compliance with the Payment Card Industry Data Security Standards.
- In addition the Council also invited the Scottish Business Resilience Centre (SBRC) to carry out an additional external vulnerability test of the Council network in 2015

1.3 The IT Health Check is conducted annually for the purposes of ensuring PSN compliance and comprises both an external and internal vulnerability test. The IT Health Check tests must be undertaken by a Government-certified organisation using Government-certified testers. This year's tests were undertaken in July by a security company called RandomStorm. The tests are procured by the Information Security team and the testing company is changed every year in line with best practice. Identified vulnerabilities are rated according to a recognised standard scoring system.

1.4 The external test involves the tester attempting to break or hack into the Council's network and all its externally facing systems, including the Council website.

1.5 The internal test involves the tester assessing 10% -15% of the Council's servers and a representative sample of PCs, laptops, etc. by running automated checks of their configurations and also trying to gain access to systems as an unauthorised user.

1.6 The outcome of the IT Health Check was positive and demonstrated that the Council's cyber security systems were safe and robust. PSN compliance requires a higher standard of security and protection than most other sectors therefore the checks carried out in this testing are more rigorous than would be undertaken by many other organisations.

The findings are summarised in the tables below with the figures from the 2014 checks included for comparison.

EXTERNAL TEST REPORT SUMMARY 2015

"Overall, the security of Perth and Kinross Council's external network is considered average when compared to similar tested networks".

Year	Critical	High	Medium	Low
2015	0	0	49*	6
2014	0	12	13	25

*NB * of the 49 Medium risks only 4 score high enough to warrant mitigation for PSN compliance*

Given the broad nature of the business of local government , the number of systems in place, the reliance on third party suppliers' application systems and the pace of change in digital technology, it is recognised that it would be impossible to ever be assessed as "risk free". In terms of the assessment the assessor has summarised the security position as "average". This is not a negative comment. It simply reflects that the issues identified are the same or similar to those faced by all other local authorities.

INTERNAL TEST REPORT SUMMARY 2015 *"The security of Perth and Kinross's internal network was of a very high standard".*				
Year	Critical	High	Medium	Low
2015	1*	3	*3*	*3*
2014	25	71	*74*	*8*
*NB * The critical risk relates to a legacy system which is in the process of being decommissioned.*				

1.7 Much of the externally facing network is dependent on third party suppliers' application systems. These often use older versions of system software which contain known vulnerabilities. The Council is generally unable to require suppliers to rectify identified issues and therefore must take steps to mitigate the vulnerabilities in other ways where possible.

1.8 Importantly, since the IT Health Check in 2014, there have been no known compromises of Council systems.

1.9 The IT Health Check report findings were passed to IT to work on mitigating the Critical, High and significant Medium risks prior to the 2015 PSN submission in September. The lower level risks will be addressed as part of ongoing maintenance.

1.10 As part of the PSN accreditation process the Government's assessors consider the outcomes of the IT Health Check and any actions taken or identified to mitigate significant vulnerabilities. They also review details of the Council's network design to ensure that they are satisfied that it meets the stringent requirements for PSN compliance.

It should be noted that the Government Assessors are satisfied with our cyber security arrangements and the Council received its PSN accreditation for 2015 on 26 November 2015.

1.11 The Council, as an organisation which can take debit and credit card payments, is also required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). A failure to comply with this standard can result in considerable financial penalties in the event of a disclosure of card details.

An external and internal vulnerability test of the network is conducted every quarter for compliance with the PCI DSS. The external test must be conducted by PCI-qualified testers and the internal test is conducted by Council staff using an approved testing tool. The Council must pass the tests to achieve compliance.

No compliance issues have been identified to date.

1.12 In addition, in May this year an additional external vulnerabiliy test of the Council network was undertaken by the Scottish Business Resilience Centre (SBRC) at the request of the Council. That test found that the Council had taken reasonable steps to ensure a secure work environment. Two technical vulnerabilities were identified in the test which SBRC considered to present a theoretical medium risk to the Council. In practice, however, it would require considerable effort to take advantage of these vulnerabilities and for that risk to be realised. Details of the vulnerabilities were passed to IT and have been appropriately mitigated.

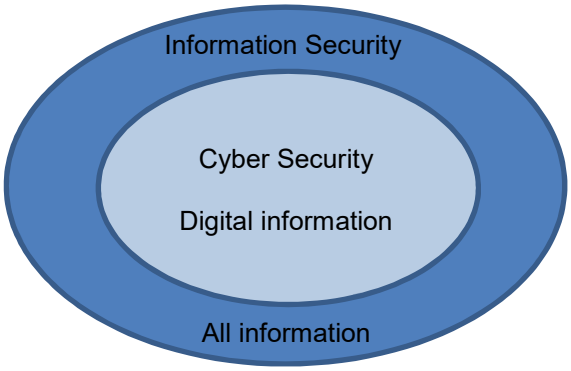
1.13 In summary, the Council has an assured, secure, government-accredited network and its security posture is robust in many areas. Systems are continually monitored internally and subject to regular external assessment. Risk and vulnerabilites as identified are passed to ICT for remedial and mitigating action. Within the context of local government, user error or abuse pose the greatest risk

1.14 It is planned to produce this report annually for the Executive Officer Team and the Committee. It will be timed to follow the Council's submission to the PSN.

2. BACKGROUND & CONTEXT

2.1 Cyber Security v Information Security

"Cyber security" is a relatively recent term which has found popularity over the last five or six years. "Cyber security" has no formal definition, but in general can be taken to mean the security measures which relate to information held digitally. This would include measures to protect the Council network - application systems, databases and computers on that network - and beyond the Council network - internet connections, mobile networks and websites.



In comparison, "Information Security" is a well-established term. Information Security relates to the security in place around ALL the Council's information irrespective of the manner in which it is stored.

2.2 Development of Information Security in the Council

The Council started working on Information Security in 1999 and has had a formal policy in respect of Information Security since 2001. The Council now has a mature Information Security Policy and a comprehensive Information Security Management System (ISMS) based on ISO 27002, the international standard for Information Security Management. The majority of the Council's Information Security standards relate to cyber security.

2.3 Cyber Security Partners

The Council's Information Security Team works closely with other Scottish local authorities, the Scottish Government and other governmental organisations through the Scottish Local Authority Security Group (SLASG).

In 2014, SLASG was formally registered with the UK Centre for the Protection of National Infrastructure (CPNI) as a Warning and Advice Portal (WARP). This provides a forum to receive and share up-to-date cyber threat information and share best practice as part of the Cyber-security Information Sharing Partnership (CiSP) under the UK's Computer Emergency Response Team (CERT-UK).

2.4 Cyber Security Threats

In general the Council is not considered to be a high profile target. Attacks against the Council are generally unsophisticated and indiscriminate, i.e. spam, phishing emails, email viruses, and probing scans.

However, the Council has been subjected to increasingly sophisticated and targeted spam, referred to as "spear phishing", where emails are specifically designed to target the Council. Prior to the actual attack, several weeks of conditioning emails are sent designed to "retrain" our spam filter to allow the malicious emails through. Whilst these attacks can be successful in penetrating our network, the risks are generally mitigated by user awareness - employees recognise the emails as suspicious and delete or report them.

The Council's profile as a target could increase rapidly however in response to local events, for example a high profile event, court case, or controversial policy decision all have the potential to make the Council a target.

In December 2015 the Council experienced degradation in its internet connection through the JANET network (which provided the Council's internet connection) as a consequence of a targeted attack on another part of the JANET network. The Council was only slightly inconvenienced by this action, although during a similar incident in 2014 several local authorities in the West of Scotland lost internet connectivity completely for several days.

This year four Scottish Councils have also been subjected to a "ransomware" attack (an attack which encrypts data and will release it only on payment of a ransom) with some limited success. Attempts have also been made to attack the Council in this way.

Local authorities are also considered to be targets for foreign national intelligence services. Information relating to these threats is limited, however, for reasons of national security.

Police Scotland will always alert local authorities where there is intelligence that suggests a potential threat to allow the Council to take preventative measures where possible. However, such intelligence is not always available.

As members of the Public Services Network (PSN), the Council is now required to develop its own threat profile to ensure continued compliance. This is a significant change in approach from PSN as regards risk management which will be reflected in our internal processes going forward.

2.5 Cyber Security and Compliance

As a local authority we are subject to various external compliance requirements in terms of our cyber and information security standards. PSN requirements and the PCI DSS have been mentioned above.

As a controller and processor of personal information, the Council must also comply with the requirements of the Data Protection Act 1998. The UK Information Commissioner's Office issues regular security guidance to ensure that organisations comply with the 7th Data Protection Principle. This requires that "*appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

The Information Commissioner has the power to serve a fixed monetary penalty notice of up to £500,000 on an organisation for a significant breach of the Data Protection Act. The majority of monetary penalties issued to other bodies to date have been for breaches of the 7th principle and have each exceeded £100,000.

3. CYBER SECURITY - POLICY, STRATEGY & GOVERNANCE

The Council's Information Security Policy is summarised in the following sentence: -

"The purpose of this policy is to ensure the confidentiality, integrity and availability of all the Council's information assets and to ensure that they are appropriately protected from all threats, whether internal or external, deliberate or accidental."

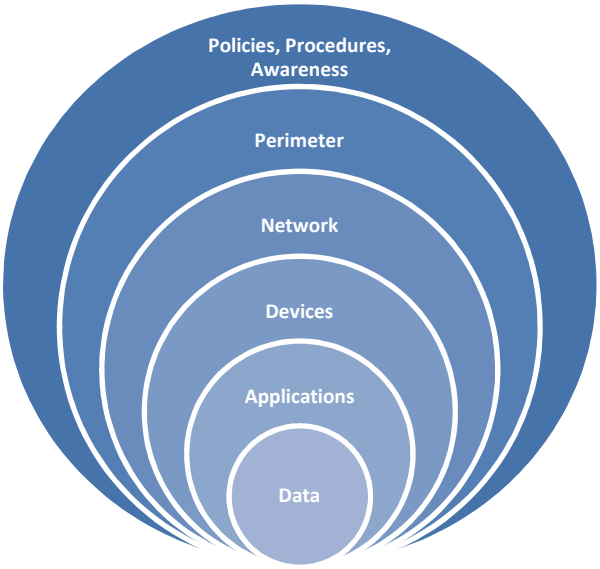
Given the continuous changes in ICT and information compliance requirements, the Council has not documented a strategy for Information Security; the general approach is to satisfy compliance requirements and best practice standards.

The Council has a designated Senior Information Risk Owner who is responsible for information security at a strategic level. The Policy and Governance Group normally acts as the senior management forum for information security, but will refer matters to the Executive Officer Team when it is considered appropriate to do so.

4. WHAT DOES CYBER SECURITY LOOK LIKE?

The Council, like all internet-connected organisations, is subject to constant, but indiscriminate, attack. The Council protects itself by having multiple layers of specialised devices and pieces of software throughout the network: a principle known as “Defence in Depth”.

These security layers are described in general terms in this section.



Cyber Security - Defence in Depth

4.1 Data

“Data” is the information to which all cyber security measures apply. This is what we aim to protect.

Information held on PCs, laptops and tablets is protected by encryption. Whilst it is possible to encrypt information held on servers, it is not feasible in many circumstances.

The weakest link in security within any organisation is the actions, omissions or errors of individuals. Staff continuously require to access and process data to carry out their roles. Certain information requires to be restricted, for example access to personal information, and it is important that the organisation has appropriate processes for authorising access to data and systems. The appropriate policies and processes are in place but, to ensure that access is properly managed, application managers and / or IT require to be kept up-to-date with details of all employees who move, start and leave the Council.

4.2 Applications

“Applications” are the programs or “apps” which run on devices. Applications normally have an additional user-id / password regime and enforce access restrictions based on the user-id.

Applications require periodic maintenance and updates. Some of these updates will be to ensure compatibility with updates to the underlying device. On occasion application updates may not be available from suppliers because their product is not ready to cope with updates to the device. In these cases alternative measures are implemented to ensure that the Council does not become vulnerable to attack through out-of-date devices.

4.3 Devices

"Devices" refer to the Council's servers and the PCs, laptops, tablets and phones used by employees. Most devices are maintained and updated regularly against published security problems. Several systems are employed solely for the task of keeping Council computers up to date.

In November 2015: -

- 12 updates were rolled out to approximately 10,000 desktop and laptop devices.

The Council's recent deployment of technology for virtual desktops and mobile devices with remote network access has reduced the complexity of the network and will also bring about a small reduction in the number of devices connecting to it. In turn, the reducing complexity increases security and flexibility.

4.4 Network

Inside the network there are further specialised systems which monitor and analyse the traffic in and out of the network. These systems look at email and internet traffic, detect viruses, and deliver secure web services to the public such as the library and online planning systems.

As stated above, in November 2015 these systems blocked: –

- 7,190 emails containing viruses
- 206,311 spam emails
- 1,066,909 malicious connection attempts
- 774 viruses and malware on the network

During that month there were no known compromises of any Council system.

4.5 Perimeter

The perimeter is the border between the Council's private network and the public internet. In 2014 it was estimated that 16 billion devices were connected to the internet in the world. The background "noise" of the internet lets malicious hackers hide and constantly scan for any weaknesses that will allow them to infiltrate and take control of vulnerable computers and network.

To defend against this the Council has security gateway devices on its perimeter, such as firewalls. These defend against hundreds of low level attacks every minute.

4.6 Policies, Procedures and Awareness

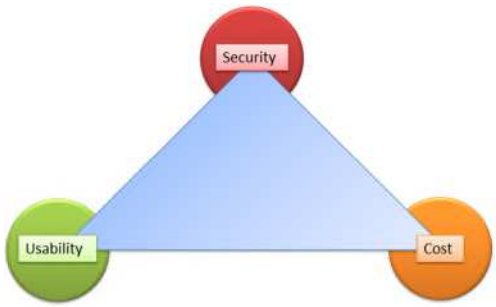
Cyber security refers to information in the digital realm, but the majority of that information will be used at some point by employees. This means that the

Council needs policies and procedures, in addition to technological controls, to manage digital information in the Council through its creation, use and destruction. Crucially, the policies and procedures also set standards for the technological controls themselves.

5. CHALLENGES

The Council has a reasonably robust cyber security posture, however, there are areas where challenges exist.

5.1 Expectation management



IT is evolving rapidly in the home. Free services are being made available that make communication and data sharing increasingly easy .New and innovative devices appear on the market every day that are both powerful and cheap. This can cause frustration when employees see the flexibility and quality of these services and devices and want to bring them into the workplace. Unfortunately, what is suitable for the home may not always be compatible with the Council's systems.

It is important to note that the Council has to take a collective responsibility for everything that touches its network and the rules (and laws) that apply to the Council as a public authority and corporate entity are different to those that apply to an individual at home. This can result in the Council appearing to be staid and inflexible when, in reality, the Council has no choice but to take a more measured and thoughtful approach to new developments in IT.

This can be particularly difficult when other organisations who work with the Council understandably take advantage of the many free products available to them and wish to use these products for the storage and movement of our information. The Council must refuse to do this because of the risks outlined above.

Unfortunately robust cyber security will almost always be in conflict with low cost and usability.

5.2 Asset Management

In order to know that all Council information assets are secure we must first know what assets we have. This can be problematic as the understanding of what is an "asset" varies across the Council.

In terms of cyber security we must consider assets to be any system or service which holds the Council's information digitally. The Council has a basic asset register and the Information Security team is working with IT currently to further improve the register and the management of our cyber assets.

5.3 Classification of Information

UK Government and the armed forces have long had a formal information classification scheme. A new, simplified Government scheme was introduced in April 2014 which means that almost all information held by local authorities should be classified at the same level.

The Council currently has no formal scheme. A scheme for the Council is currently under discussion which would differentiate between publicly-available information and more sensitive information whilst still aligning with the Government scheme.

5.4 Flexible and Mobile Working

Flexible and mobile working is part of the Council's strategic direction. Compliance requirements from PSN have required a radical move away from the use of personal devices for work purposes (BYOD – Bring Your Own Device) to only using Council-owned devices. Although this may appear to be a backwards step, in fact choosing to use Council-owned mobile devices significantly improves support issues as well as our cyber security.

The topology of Perth and Kinross as a region and the rural nature of much of the authority will always present problems in terms of mobile data access. While the government's ambition is for comprehensive high speed mobile internet coverage (i.e. 3G, 4G and beyond), this will not always be possible in remote areas.

PSN compliance requirements will continue to present difficulties in the use of free public Wi-Fi in cafés and public spaces as an alternative form of connection for mobile working. Work is currently being undertaken to implement a partial solution to this problem.

5.5 User Awareness and Education

People will always be the weakest link in any secure system. Employees have authorised access through physical security measures and have passwords and access rights to permit access through cyber security measures. They can breach security accidently or deliberately, naively or maliciously.

Some employees with significant authority on the network or in the Council must be considered potential targets of malicious organisations; these would include system administrators within IT, procurement specialists, and finance staff. Even staff with significant physical access to Council buildings at quiet times (such as cleaners) can be considered potential targets.

Educating users in what the Council's policies and standards are can help reduce the number of security incidents that occur. Security can be a dry topic and awareness programmes need to be innovative to attract and hold attention. Training programs also need to evolve to ensure employees are receiving

training that is up-to-date with current threats. Managers and risk owners could benefit from specific additional training to increase their awareness of the impact their decisions can make.

Little can be done to prevent an employee's actions that are both deliberate and malicious. Pre-employment checks can help screen out criminal infiltration, but sophisticated automated monitoring of the network (known as protective monitoring) is required to detect and stop malicious actions when they occur.

5.6 Protective Monitoring

Protective monitoring is the process through which Council systems are constantly scrutinised for changes that might indicate a problem. Most Council systems are capable of generating logs of their activities. These logs can be examined manually or by special systems which look for changes in the pattern of activity. The Council's systems are capable of creating colossal amounts of information - millions of log entries an hour - with the result that the Council currently struggles to interpret or even store monitoring information for any practical period of time. Firewall logs, for instance, are overwritten very quickly due to the volume of recorded events. Ideally activity logs should be retained for six or even twelve months.

Moving forward the Council is considering a sophisticated protective monitoring system. Enquiries have been made regarding a local authority consortium procurement of such a solution, however protective monitoring remains a difficult and expensive function to carry out to a good standard. Protective monitoring in some form is a requirement of both our PSN Code of Connection and the PCI DSS standards.

5.7 Changing Compliance Standards

Historically, the principal standards that have driven the Council's security compliance have come from the PSN. With the move to self-assessment in terms of identifying threats for PSN the onus is now placed on the Council to both determine and justify most of the security standards it adopts.

To satisfy this requirement, a cyber security threat profile was developed in 2015 and a risk assessment was undertaken based on it using a UK Government standard process. The resulting document provides a lengthy and very technical analysis of all the potential cyber security risks facing the Council.

These potential risks were matched against the existing controls and the residual risks consolidated into three key areas. All three areas are already the subject of improvement activities which will provide adequate levels of control in these areas.

The threat profile and risk assessment will be reviewed periodically as necessary.

The PCI DSS changed quite significantly in 2013 and it remains very prescriptive, unlike the current PSN requirements. This remains a compliance challenge for the Council.

6. FUTURE DEVELOPMENT OF CYBER SECURITY

6.1 The demands placed on cyber security are continually changing as technology and its use changes. As a consequence, the Council's cyber security measures must continually develop and change.

6.2 The following are some of the areas in which developments are currently in progress or are planned for the current year: -

1. Development of a standard risk assessment process / template for application systems
2. Further development of information security awareness material
3. Retention and management of system activity logs
4. Improvements related to security in the process for the procurement of new IT systems

7. CONCLUSION AND RECOMMENDATIONS

The Council has an assured, secure, government-accredited network.

The Council network is subject to ongoing and evolving cyber-attacks which, to date, have been successfully rebuffed. The Council network must continuously evolve with the threats in order to remain secure. Challenges are faced in continuing to provide a secure network which is flexible in the face of demands for new working styles from inside the Council and the increasing need to work in partnership with other organisations who have different security postures.

The Council's security posture is robust in many areas but has areas for improvement, particularly protective monitoring and user awareness. It is not possible to secure anything completely, so detection can be as important as prevention.

The Committee is asked to:

1) Note the content of the report.

2) Instruct the Head of Legal and Governance Services to bring forward an annual report on cyber security following the Council's submission to PSN each year.

Author(s)

Name	Designation	Contact Details
Donald Henderson	Information Compliance Manager	Ext. 77930

Approved

Name	Designation	Date
John Walker	**Depute Chief Executive**	**19 January 2016**

If you or someone you know would like a copy of this document in another language or format, (on occasion, only a summary of the document will be provided in translation), this can be arranged by contacting the Customer Service Centre on 01738 475000.

You can also send us a text message on 07824 498145.

All Council Services can offer a telephone translation facility.

ANNEX

1. IMPLICATIONS, ASSESSMENTS, CONSULTATION AND COMMUNICATION

Strategic Implications	**Yes / None**
Community Plan / Single Outcome Agreement	**None**
Corporate Plan	**None**
Resource Implications	
Financial	**None**
Workforce	**None**
Asset Management (land, property, IST)	**None**
Assessments	
Equality Impact Assessment	**None**
Strategic Environmental Assessment	**None**
Sustainability (community, economic, environmental)	**None**
Legal and Governance	**Yes**
Risk	**None**
Consultation	
Internal	**None**
External	**None**
Communication	
Communications Plan	**None**

1. Strategic Implications

Community Plan / Single Outcome Agreement

1.1 Not applicable

Corporate Plan

1.2 Not applicable

2. Resource Implications

Financial

2.1 Not applicable

Workforce

2.2 Not applicable

Asset Management (land, property, IT)

2.3 The Head of Finance and Support Services, Housing and Community Care has been consulted and has indicated agreement with the report.

3. Assessments

Equality Impact Assessment

3.1 The proposals have been considered under the Corporate Equalities Impact Assessment process (EqIA) and assessed as not relevant for the purposes of EqIA.

Strategic Environmental Assessment

3.2 The Environmental Assessment (Scotland) Act 2005 places a duty on the Council to identify and assess the environmental consequences of its proposals. However, no action is required as the Act does not apply to the matters presented in this report. This is because the Committee are requested to note the contents of the report only and the Committee are not being requested to approve, adopt or agree to an action or to set the framework for future decisions.

Sustainability

3.3 Not applicable

Legal and Governance

3.4 Part of the Governance framework.

Risk

3.6 Not applicable

4. Consultation

Internal

4.1 Not applicable

External

4.2 Not applicable.

5. Communication

5.1 Not applicable

6. BACKGROUND PAPERS

None.

7. APPENDICES

None.