PERTH AND KINROSS COUNCIL

Strategic Policy and Resources Committee

18 April 2018

ANNUAL REVIEW OF CYBER SECURITY

Report by 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 is transacted and managed digitally. Information is a key business asset which needs to be protected. This report provides a description of the current arrangements in place within the Council 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.

1.2 By way of context, during February 2018 the following threats were identified:-

- 683,367 blocked emails (Spam, phishing, content type and malware)
- 398,416 malicious connection attempts
- 18 viruses and malware on the network

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

1.4 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.

1.5 The annual IT Health Check is conducted for the purpose 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. 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.

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

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

1.8 The outcome of the IT Health Check in June 2017 was positive and demonstrated that the Council's cyber security systems were safe and robust.

1.9 The external test, which looks at the public exposure of the network, identified only one low risk vulnerability.

1.10 The internal test did discover a number of nominally high risks, however since these risks only manifest inside the corporate network they are manageable and actions to reduce these identified risks have been taken.

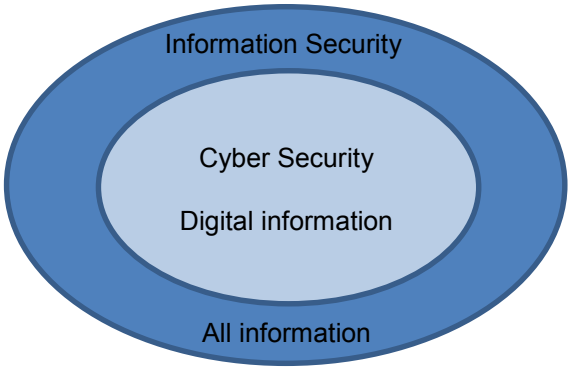
1.11 In 2017 the information security team ran four email phishing simulations. These tests highlighted user awareness as an area for improvement. Click rates for phishing emails reached 25% which equates to 1 in 4 of our users being susceptible to email phishing scams.

1.12 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 IT for remedial and mitigating action. Within the context of local government, user error or abuse poses the greatest risk.

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.



2.2 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.

Development of Information Security in the Council

2.3 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.

Cyber Security Partners

2.4 The Information Security team works closely with other Scottish local authorities, the Scottish Government and other government organisations through the Scottish Local Authority Information Security Group (SLAISG).

2.5 The Council is also a member of the Cyber Information Sharing Portal (CISP) which is managed by the National Cyber Security Centre (NCSC).

Cyber Security Threats

2.6 The Council is not considered to be a high profile target. Attacks against the Council are generally indiscriminate, i.e. spam, phishing emails, email viruses, and probing scans, but the sophistication of these attacks is increasing rapidly. The NHS, local authorities and other public sector bodies are now regularly reported as being affected by cyber-attacks, most notably continuing ransomware attacks.

2.7 The Council has invested in new technology in an attempt to block more of these attacks from entering the network. No technological measure is 100% effective and ultimately we must depend on our staff being vigilant to those malicious messages which make it through our defences. The Council has also purchased a product to carry out simulated phishing attacks against our employees. These simulations allow employees to be exposed to superficially malicious emails and providing an element of awareness education to those who fall for the ruse without any danger to the network.

Cyber Security and Compliance

2.8 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.

2.9 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.*"

2.10 In May 2018 the Council will be expected to comply with the new UK Data Protection Act which will implement the EU General Data Protection Regulation in UK law and will supersede the existing legislation. The security requirements set out in the new legislation are similar to the existing 7th Principle, but are more specific and will require careful attention.

3. CYBER SECURITY - POLICY, STRATEGY & GOVERNANCE

3.1 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."

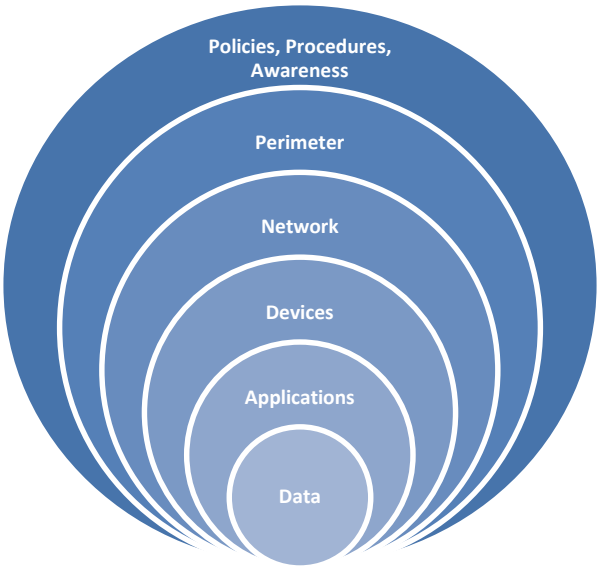
3.2 Given the continuous changes in ICT and information compliance requirements, the Council has not documented a strategy for Information Security; the general approach is to satisfy compliance requirements and best practice standards.

3.3 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

a. 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.

b. 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 have to be implemented to ensure that the Council does not become vulnerable to attack through out-of-date devices.

c. 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.

The Council's 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.

d. 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 February 2018, these systems detected and blocked: –

- 683,367 blocked emails (Spam, phishing, content type and malware)
- 398,416 malicious connection attempts
- 18 viruses and malware on the network

There were no known compromises of any Council system since the last review report in 2017.

e. 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 across the world and it is predicted that by 2020 this will be 30 billion devices. 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.

f. 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.

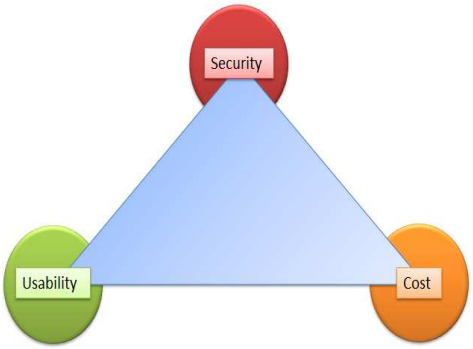
5. CHALLENGES

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

a. Grey Procurement

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 requirements.

Many of these services and products can be accessed using nothing more than an internet browser. As a result, it is possible for Council operational units to procure these services without reference to IT and without considering the potential security impact, and also in breach of procurement and data protection.



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.

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

b. 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.

c. 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 classification scheme.

d. 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.

The email phishing simulation used an online system to imitate common phishing email scams. If users fell for the fake emails rather than being taken to a malicious website they were presented with user awareness materials.

Initial tests, which imitated internal emails from IT, had click rates of around 25%. This unfortunately means that one in four of our staff when presented with a similar but malicious email would be at risk of clicking on its links and introducing malware into the council network.

More promisingly a test conducted in December 2017 which imitated Christmas offers from well-known companies had a click rate of only 6%. This indicates that staff are appropriately suspicious of spam type emails but that more work is needed to make internal emails more recognisable and to increase our employees awareness of potential malicious emails.

e. Changing Compliance Standards

Historically, the principal standards that have driven the Council's security compliance have come from the PSN. Following a series of ransomware attacks which affected the NHS in Scotland, the Scottish Government have accelerated their national Cyber Resilience programme and want to extend this across the public sector.

At first reading, the requirements appear to create some degree of duplication and work is currently being undertaken to assess the implications of the programme for the Council. This will be the subject of a further report to the Executive Officer Team.

6. FUTURE DEVELOPMENT OF CYBER SECURITY

a. 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.

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

1. Refinement of an application risk assessment process to identify significant risks within existing high value applications systems.
2. Continued development of a cyber awareness programme
3. Ensuring that we get best value from the security technologies already within the Council network.
4. Contributing to the Cyber discussion between local authorities, Scottish Government and NCSC.
5. Review of the Council's Information Security Policy.

7. CONCLUSION AND RECOMMENDATIONS

7.1 The Council has an assured, resilient, government-accredited network.

7.2 The Council network is subject to ongoing and evolving cyber-attacks. Although a small number of these attacks have breached the network perimeter the response plans in place have allowed the incidents to be resolved quickly with minimal disruption and no compromise of confidentiality. The Council network needs to continuously evolve with the threats in order to remain secure.

7.3 The Committee is asked to:

1) Note the content of the report.

Author(s)

Name	Designation	Contact Details
Paul Dick	Information Security Officer	01738 475000

Approved

Name	Designation	Date
Jim Valentine	Depute Chief Executive (Chief Operating Officer)	16 March 2018

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

3.5 Not applicable

4. Consultation

Internal

4.1 Not applicable

External

4.2 Not applicable.

5. Communication

5.1 Not applicable

2. BACKGROUND PAPERS

None.

3. APPENDICES

None.