PERTH AND KINROSS COUNCIL

Scrutiny Committee

12 June 2019

ANNUAL REVIEW OF CYBER SECURITY

Report by Head of Legal and Governance Services (Report No. 19/180)

PURPOSE OF REPORT

This report provides an overview of Cyber Security in the Council and provides assurance as to current risks and threats. It provides an updated description of the current arrangements in place within the Council to protect that information ("cyber security") and details the relevant compliance frameworks which the organisation is subject to. It also 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. EXECUTIVE SUMMARY

1.1 The Council is continuing to move its business functions into the digital domain in line with the general trend of "digital first" seen across the public, private and third sectors. The Council's digital assets are increasingly being held within systems and services located in, and managed by, external suppliers; sometimes referred to as 'the cloud'.

1.2 The Council has updated much of its cyber security technology in the last twelve months making it difficult to provide comparable statistics to previous years. However to provide some context, in April 2019:

- 3.3 Million emails were sent and received
- 59% (1.95 Million) were stopped for various reasons; the vast majority of these were incoming emails
- 295 viruses were detected on the network (all were neutralised without incident)

1.3 The Council has not suffered a reportable incident or any network compromise since the last report in 2018.

1.4 As well as the continuous monitoring of the Council's cyber security by the Information Security team and IT Division, the security arrangements of our digital information are also subject to external reviews and assessments.

1.5 An annual IT Health Check is conducted for the purpose of ensuring Public Sector Network (PSN) compliance and comprises both an external and internal vulnerability test. This must be performed 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 a sample of 10% (over 700) 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 March 2019 was positive with the tester stating, "The overall security of the environment was of a good standard".

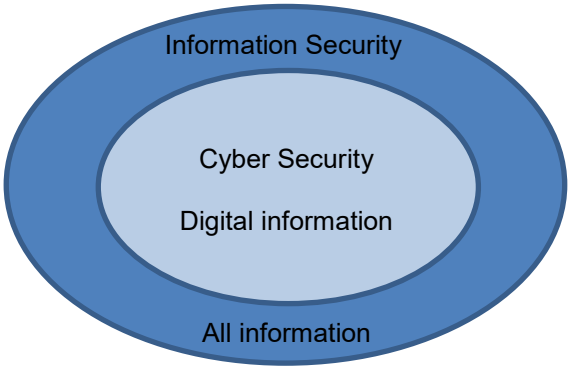
1.9 The internal test did identify a number of high risks, however since these risks only manifest inside the corporate network they are manageable and actions to reduce these identified risks have been taken. Many of the identified high risks related to patching and remedial actions were already scheduled as part of business as usual within IT.

1.10 In summary, the Council has an assured, secure, independently 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

Cyber Security v Information Security

2.1 "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.

2.4 Funding has been awarded by the Scottish Government for the employment of a cyber security trainee for a period of twelve months. The trainee will undertake duties within both Legal & Governance Services and IT to assist with risk assessments, security policy and governance, and extending the use of existing security technologies. The individual will be offered a recognised cyber security qualification as a condition of the funding award. No recurring funding for this role has been identified at this time.

Cyber Security Partners

2.5 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).

2.6 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

2.7 The cyber threats levied against the Council have largely remained the same over the last 12 months. Large scale nation state attacks from Russia, North Korea and China are continuing to make headlines in the press. Although the Council is not a specific target of hostile nation states there is always a possibility that damage and disruption can be caused indirectly in the same way the NHS was adversely affected by the WannaCry malware; now publicly attributed to North Korea.

2.8 Ransomware and phishing attacks, also well reported in the press, are carried out by serious organised crime groups. These attacks are again unlikely to target the Council directly but damage and disruption can still occur if these attacks spread and are able to gain a foothold into the Council network.

2.9 The overall risk to the Council from malicious agents remains relatively moderate as long as basic cyber hygiene is maintained. This includes keeping systems maintained and up to date with security patches and updates. The Council's IT service has a well-established and robust patching routine however it is important that Services understand that these updates do require occasional system downtime.

Cyber Security and Compliance

2.10 The Council continues to be subject to various external compliance requirements in terms of our cyber and information security standards. The Public Sector Network (PSN) is a connection required by the Council for critical business functions including Housing Benefits, Registrar services and Blue Badges. The Council must reaccredit to the PSN annually and provide assurance that the Council network is well run and presents no onward risk to central government services.

2.11 The Council is currently going through the reaccreditation process for its 2019-20 PSN connection.

2.12 The Scottish Government has requested that local authorities accredit to the Cyber Essentials scheme in addition to the PSN. In 2018 the Council accredited to Cyber Essentials Basic and in 2019 is currently accrediting to the higher Cyber Essentials Plus scheme. This is being done in parallel to PSN accreditation.

2.13 The Council is also required to accredit to banking regulations associated with credit and debit card payments specifically the Payment Card Industry Data Security Standard (PCIDSS). A significant amount of work has already been done to allow the Council to meet the compliance requirements of the PCIDSS and it is expected that the Council will be accredited to that standard by the end of 2019.

2.14 As a controller and processor of personal information, the Council must also comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The UK Information Commissioner's Office issues regular security guidance to ensure that organisations comply with the appropriate articles of the GDPR. Information security is significantly more prominent within the GDPR legislation than the previous 1998 Data Protection Act.

2.15 The Council has also been required to complete the Scottish Government's Public Sector Cyber Resilience Action Plan (PSAP). As mentioned earlier, this includes compliance with the Cyber Essentials certification scheme but also the adoption of Active Cyber Defence services and alignment with Scottish Government incident reporting procedures.

2.16 Active Cyber Defence services are provided by the NCSC and include –

- Webcheck – a service to check the basic health of Council websites. This service is currently monitoring 94 Council websites on a daily basis
- Mailcheck – a service which helps prevent the Council's email addresses being spoofed for malicious intent.
- Protective DNS – Providing an additional layer of security to defend against malicious websites

2.17 These services are free for the Council to use.

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 The policy was reviewed by the Policy and Governance Group in February 2019.

3.3 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.

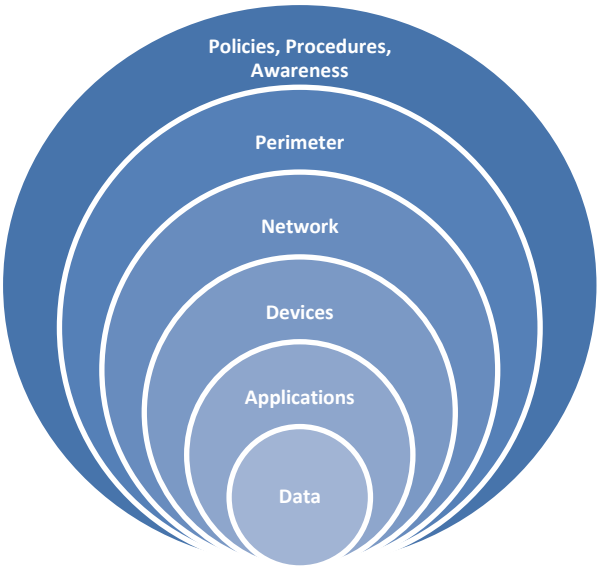
3.4 The Council has a designated Senior Information Risk Owner (SIRO) who is responsible for information security at a strategic level. The Council's SIRO is Jim Valentine, Depute Chief Executive and Chief Operating Officer.

3.5 The Policy & Governance Group normally acts as the senior management forum for information security, but will refer matters to the Corporate Management Group or 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

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

4.1.2 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.

4.1.3 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

4.2.1 “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.

4.2.2 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.

4.3 Devices

4.3.1 “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.

4.3.2 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.

4.4 Network

4.4.1 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.

4.4.2 There were no known compromises of any Council system since the last Cyber Security report in 2018.

4.5 Perimeter

4.5.1 The perimeter is the border between the Council's private network and the public internet. In 2018 it was estimated that 23 billion devices were connected to the internet across the world and it is predicted that by 2025 this will be 75 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.

4.5.2 As the Council moves towards 'cloud' based services, its perimeter will cease to be a recognisable wall around its physical assets. The Council's perimeter will extend into the internet itself and actually become part of the internet. The technologies and services the Council uses are changing and adapting to ensure that Council information is protected both inside the physical walls of its buildings and within the digital walls of its cloud services.

4.6 Policies, Procedures and Awareness

4.6.1 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.

5.2 Grey Procurement

5.2.1 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.

5.2.2 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 policy or legislation.

5.2.3 Not all of the demand for these services is internal, much of the pressure to utilise these services is driven by external bodies who wish to utilise them for their own purposes without consideration for their stakeholders. File sharing websites such as Dropbox are now required by services within the Council but without any technical mechanism to control accounts and access. Currently approximately 170 employees have uncontrolled access to file sharing websites. The risks associated with that access have been accepted by line management but investigations are underway to identify better ways of working to reduce these numbers.

5.2.4 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.

5.2.5 Robust cyber security can often conflict with requirements for low cost and usability, however; the Information Security Team will always endeavour to find effective business-focussed solutions to security issues.

5.3 Classification of Information

5.3.1 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.

5.3.2 The Council currently has no formal classification scheme.

5.4 User Awareness and Education

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 IT has implemented a technology which will help to detect malicious actions within the network. Security Incident and Event Monitoring (SIEM) technology can detect patterns and action which can be highlighted to relevant members of staff. This technology continues to be developed to refine its capabilities.

5.4.5 The phishing exercises carried out in 2017 highlighted a weakness in employee's knowledge of the types of email based threats that exist. Information security intends to recommence phishing simulations utilising the license-free software "Go Phish" to reduce the level of this threat.

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: -

- Management of risk with cloud-based developments particularly the use of the Microsoft Office 365 suit of tools
- Continued development of a cyber awareness programme particularly the use of phishing simulation software
- Recruitment of a Cyber Security Trainee
- Contributing to the Cyber discussion between local authorities, Scottish Government and NCSC.
- On-going review of the Council's Information Security Policy and Standards.

7 CONCLUSION AND RECOMMENDATIONS

7.1 The Council continues to have an assured, resilient, independently accredited network.

7.2 The Council network as a large and trusted organisation is regularly and repeatedly subjected to attacks from external agents. In the previous 12 month period Council defences have successfully prevented any significant breaches of Council digital assets. Attacks against the Council are constantly evolving and preventative measures must also evolve to keep pace with these threats.

7.3 A move to cloud based services such as Office 365 will present new challenges to the Council and our defensive technologies and employee training must change to allow the benefits from these services to be fully realised.

7.4 It is recommended that the Scrutiny Committee: -

(i) Consider and comment on this report
(ii) Note the content of this report

Author(s)

Name	Designation	Contact Details
Paul Dick	Information Security Manager	01738 475000

Approved

Name	Designation	Date
Jim Valentine	Depute Chief Executive (Chief Operating Officer)	13 May 2019

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.

ANNEX

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.