HERTFORDSHIRE COUNTY COUNCIL

Agenda Item No.

3

AUDIT COMMITTEE
FRIDAY 7 JULY 2017 AT 10.30 AM
RISK FOCUS REPORT – CYBER SECURITY

Report of the Director of Resources

Author: Dave Mansfield, Head of Technology (Tel: 01992 588331)

Executive Member: David Williams – Resources, Property & the Economy

1. Purpose of report

1.1 To provide further information regarding the risk and associated controls recorded on the Hertfordshire County Council Corporate Risk Register relating to Cyber Attack Risk (TEC0004), "In the event of failing to maintain and ensure the use of Hertfordshire County Council's security systems, technical protocols and change management processes, there is a risk of a cyber-attack (virus, penetration or malicious internal action) on the County Council's ICT environments causing significant service disruption and possible data loss."

1.2 This report invites the Audit Committee to endorse the overall approach that Hertfordshire County Council is taking to mitigate this risk. In addition, it seeks support in recommending some additional technical measures and resources be procured to meet the increasing and evolving cyber-attack risk. In considering these matters, ICT Technology have considered various industry sources including Ernst and Young in their recent papers on Ransomware and wider industry guidance.

2. Summary

2.1 All computer systems and the information contained therein are at risk of being compromised in a variety of ways. This may be through malicious or accidental actions, or simply through the failure of software or electronic components. Whilst all of these potential risks are considered a "Cyber- Attack", a malicious attack from the Internet is the main focus of the risk being addressed in this paper. It is an issue that is currently hitting the headlines as well as something that could potentially lead to both actual and reputational damage for Hertfordshire County Council. A recent ransomware outbreak affected Hertfordshire County Council's close working partners in the NHS and for the wider industry this is a timely reminder of this increasing risk.

2.2 The County Council is seeing an exponential increase in the number of attempted cyber-attacks from the internet. These take the form of:

- Automated and manual scans for weakness on Hertfordshire County Council's public facing perimeter defences;
- Attempts to flood Hertfordshire County Council's network with false requests so that Hertfordshire County Council's ICT services fail to operate and affect Hertfordshire County Council's ability to deliver public services; and
- Delivering realistic looking emails with ransomware and other malicious payloads (virus, ransomware and malware attacks) as well as the 'traditional' scam attempts.

2.3 In mitigating against this risk ICT Technology seeks to ensure that:

- The best technical defences are in place;
- Hertfordshire County Council's systems and software are kept up to date (witness recent NHS issues) ;
- Hertfordshire County Council staff are aware and alert to the possibility of threat and act accordingly;
- If/when an attack is encountered, ICT Technology act quickly and lockdown/ quarantine/ contain that threat.

2.4 Hertfordshire County Council continues to follow industry best practice and apply any lessons learnt. ICT Technology have combined elements of ISO Security Standards (ISO 27001:2013) with central government security framework guidance and applied these in a pragmatic and effective manner. In general, this has led to the application of multi-layered security defences. Deploying secure gateways, quarantine regimes, and selecting best of breed technologies. ICT Technology have kept infrastructure and computing devices patched and current. Hertfordshire County Council have used strong encryption and strong authentication methods together with active device management in line with best practice for local government as articulated under Public Services Network (PSN) accreditation regime.

2.5 Hertfordshire County Council understands the risk associated with human error, devising and disseminating user guidance and policy. ICT Technology actively monitors misuse and accidental infringement and follow up any instances with departmental managers.

2.6 Hertfordshire County Council undertakes an annual PSN (Public Sector Network) accreditation exercise to ensure it can safely connect to the PSN to deliver various services to public. This is a stringent regime set out by the cabinet office that aids Hertfordshire County Council in maintaining standards. As a part of this exercise, Hertfordshire County Council undertakes various security penetration exercises which act as independent verification of ICT Technology security measures. Hertfordshire County Council has always achieved the accreditation and is currently accredited to May 2018.

2.7 Hertfordshire County Council's IT and user support partners are a crucial part of its response to security incidents. ICT Technology have agreed

rapid response processes with associated procedures in place ICT Technology management of end user computing devices is robust and includes strict authorisation controls. ICT Technology operates an industry standard change control regime and all changes to the IT environment are assessed and need approval before they proceed. The recent global ransomware event did not affect Hertfordshire County Council due to its management approach combined with a detailed response to taking appropriate measures against the developing worldwide threat.

2.8 Hertfordshire County Council currently spends approximately £600K on all aspects of security. Network provision, accreditation, monitoring, and security testing. This is also supported by activity and responses in major IT & networking contracts.

2.9 Hertfordshire County Council have a "smart working" connected workforce that needs access to the internet to provide innovative, effective services to its clients in a timely manner. Under these conditions Hertfordshire County Council needs to be prepared to resist attack as far is possible but then also be prepared to respond to attacks that are successful in penetrating its front-line defences. Hertfordshire County Council needs to prevent, detect, contain and eradicate the attack to prevent any exposure of its data, systems or effect on its services.

2.10 The new data protection regime (GDPR- General Data Protection Regulation) will raise the bar in terms of requirements on organisations abilities to track and control data leakage whether it is via staff error or by malicious action. Penalties under the new regime potentially run into millions of pounds for organisations of Hertfordshire County Council's size.

2.11 Despite ICT Technology's success and best practice approach the increasing level of this threat means that it needs to continue to learn and increase the professional expertise, staff awareness and technological defences. ICT Technology are therefore looking to make the following additional improvements:

2.11.1 Significant Investment in multiple layers of new technology that provide defence in depth right from the edge of the network to the equipment staff use to provide services to the public.

2.11.2 Investment in a dedicated real time security monitoring facility to give ICT Technology greater automated real-time view of its security status. Hertfordshire County Council needs this emerging industry practice to be able to activate elements of its response at an earlier stage against increasingly sophisticated cyber-attacks.

2.11.3 Investment in additional skilled IT security support staffing to get the maximum out of the above technical investments and for closer management of Hertfordshire County Council's security environment.

2.11.4 Ensuring further controls on IT purchasing to avoid the rise of 'Shadow IT' that is emerging in many large organisations of similar size adding to the overall risk profile. The NHS attack has shown the vulnerability of services where unsupported IT is in place.

2.11.5 An improved and effective council wide security awareness programme for all staff with mandatory data protection and security training for all employees. A combination of e-learning and security awareness assessment tools such as those that gauge user understanding by, for instance, sending mock phishing attack email.

2.12 In summary, Hertfordshire County Council has sound and effective measures in place for the protection and management against cyber-attack. Those measures include appropriate defences, up to date patched IT infrastructure and mechanisms to heighten staff awareness. Hertfordshire County Council has applied the learning from industry specialists, best practice approaches and learning from real-life incidents such as those that impacted Lincolnshire County Council and the NHS. However, as the threat continues to increase and methods of the criminals involved adapt, ICT Technology have planned improvements and investments being made which will look to keep Hertfordshire County Council as well protected as possible against this continuously evolving threat.

3. Recommendation/s

3.1 The Audit Committee is invited to note and comment on the information provided within this report.

4. Background

4.1 The risk was first recorded in January 2009 when it became clear that the risk of a cyber-attack was emerging and that Hertfordshire County Council needed to ensure it had effective prevention and response mechanisms to:

i) ensure best practice controls and measures and
ii) take measures including staff awareness to avoid becoming victims of cyber-crimes.

4.2 Hertfordshire County Council's primary focus back then was to ensure that its technical perimeter defences were effectively maintained and tested for vulnerabilities and that ICT Technology took appropriate action to control these vulnerabilities. Cyber-attacks then focussed on the perimeter of a network.

4.3 The control measures were recorded and actioned as:

4.3.1 Industry approved security measures (firewalls, desktop AV, email filtering software etc.) implemented, monitored and maintained

4.3.2 New/updated systems/apps conform to agreed security requirements Inc. successful network penetration tests before implementation

4.3.3 A rolling program of testing network infrastructure Inc. penetration testing for Hertfordshire County Council and key 3rd party providers

4.3.4 Work to continuously develop & deliver ICT policy/security education/awareness training for staff, managers and members

4.3.5 Regular meetings with other local authorities and participation in security forums exchanging security information and learning from the experiences of others such as the cyber-attack on Lincolnshire's ICT facilities.

4.3.6 Ensure ICT Service Providers adhered to security & tech standards in providing/implementing/updating systems; ICT infrastructure. ICT Technology does actively engage with industry suppliers by attending workshops. Seminars and product demonstrations.

4.4 These controls were and are still applied with vigour and arising out of the recent attack that affected the NHS so heavily ICT Technology reviewed the status of the emerging threat, enacted quarantine processes and additional controls. Acting with all caution and then reviewing and relaxing if industry advice was showing a reduced risk. However, the exponential increase in threats from the internet combined with cloud based working, along with a significant increase in collaborative smart-working approaches, mean that these measures are in constant need of revision and investment.

4.5 A programme of work and investment are therefore planned to meet this elevating level of risk.

5. Supporting Information

5.1 The corporate risk is owned within the Resources Directorate by the Head of Technology with elements of the wider risk spanned across the organisation.

5.2 Controls are co-ordinated by staff within the Technology Department and are intended to protect and reduce the impact of a cyber-attack. The controls operate in defensive layers beginning from the physical network perimeter to logical staff access to Hertfordshire County Council's data.

5.3 All the controls set out in the table in appendix 1 have been reported through the quarterly corporate risk review process as in progress.

5.4 Key achievements to date:

5.4.1 Achieving PSN accreditation status year on year since the accreditation was introduced in 2008 for a very large and complex ICT estate.

5.4.2 Establishing staff information pages on Hertfordshire County Council's Intranet and developing a monitoring regime that allows the organisation to take appropriate action where front line staff are acting inappropriately.

5.4.3 Established a good 'track record' defending against ever evolving threats and an equally good record against electronic data loss

5.4.4 Maintaining levels of investment and supplier engagement over years to provide stable controls

5.4.5 Not being affected by major cyber-attack events that have adversely affected others in the industry, mainly by taking quick, robust and decisive preventative actions.

6. APPENDIX 1

CORPORATE RISK REGISTER		
Risk Number	**Risk Owner**	**Department**
TECH0004	Dave Mansfield	Resources
Date risk first included on risk register	**Risk treatment (response) to manage the risk**	**Executive Member**
2009	Reduce	David Williams

Description of the risk
In the event of failing to maintain and ensure the use of Hertfordshire County Council's security systems, technical protocols and change management processes, there is a risk of a cyber-attack (virus, penetration or malicious internal action) on Hertfordshire County Council's ICT environments causing significant service disruption and possible data loss

Consequences of the risk
Disruption of services, public services may be affected, reputational damage and consequential recovery costs

Current controls

TEC0004/001
Industry approved security measures (firewalls, desktop AV, email filtering software etc.) implemented, monitored and maintained.

"ICT Technology are currently actively investigating and evaluating the use of products on the market to provide up to date and additional security against malware and wider threats".

TEC0004/002
New/updated systems/apps conform to agreed security requirements including successful network penetration tests before implementation.

"SEAM and SOLERO, two schools applications were security tested with the intention of making these available over the internet to the schools. Primary Public facing applications services RBA3, email gateways, sFTP sites were subject to systems penetration tests and follow up hardening measures".

TEC0004/003
New/ updated systems/ apps conform to agreed security requirements including successful network penetration tests before implementation.

"Work to continuously develop & deliver ICT policy/ security education/

awareness training for staff, managers and members. New Members policy and staff Acceptable Use policy agreed are being published."

TEC0004/004
Rolling program of testing network infrastructure including penetration testing for Hertfordshire County Council and key 3rd party providers.

"PSN infrastructure tests and follow-up actions completed. Highways control room security vulnerabilities pen test carried out and follow-up actions being planned".

TEC0004/005
Ensure ICT Service Providers adhere to security & tech standards in providing/implementing/updating systems; ICT infrastructure

"New Questionnaire using Government's security framework guidance on Cloud Hosting has been developed, for use with cloud hosting. Next steps are to integrate these security assessments into standard supplier questionnaire. Use of vulnerability tools workshops for Serco are underway "

Current Risk score based on effectiveness of current controls		
Probability score:	***Impact score:***	***Overall score:***
4 - Likely	8 – High	32 - Severe
Reason for inclusion on Corporate Register		
The risk met the corporate risk criteria; in particular, there are significant financial implications.		
Direction of travel *(overall risk score for previous three quarters)*		
32	32	32
Target risk score		
Probability score:	***Impact score:***	***Overall score:***
3 – Possible	4 – Medium	12 – Significant