Nottinghamshire County Council

Report to Audit Committee

8 March 2017

Agenda Item: 4

REPORT OF THE SERVICE DIRECTOR, ICT

CYBER SECURITY UPDATE

Purpose of the Report

1. To provide the Audit Committee with an update on the approach taken to mitigating and managing cyber-attacks.

Information and Advice

Background

2. The County Council operates a large and complex technology estate that supports users to access more than 600 applications over cabled, wireless, 3G and 4G networks. More than 11,000 devices (desktops, laptops, tablets and smartphones) connect via these networks and services are available to front-line services every day of the year. Many users are provided with technology to work flexibly from their home, in transit or with customers and many would become unproductive very quickly without these services. The corporate ICT network also delivers the printing and telephony services for most users. The public also increasingly access and transact a wide range of County Council services online. ICT Services therefore deploys a considerable infrastructure across two data centres to manage the technology estate and provide a measure of business continuity.

3. The availability of ICT solutions and the security of information is therefore an essential component in facilitating efficient and effective day to day service delivery. The County Council collects, processes and stores huge volumes of data electronically. This data can be stored in various locations such as in e-mails, on file servers, on devices and in back-up systems. Increased partnership working requires a lot of personal and sensitive information to also be made available across organisational boundaries. All of this requires robust security practices to protect the Council, its staff, customers and partners from an ever changing range of ICT security threats.

4. Balancing security with service delivery is a complex task. Whilst security of information and services is critical, the level of security should not be so intrusive as to disrupt services. The 3 key principles of information security are confidentiality, integrity and availability:

    - **Confidentiality:** Ensures that information can only be accessed by people authorised to do so. This is the principle of information security that is most at risk and most likely to incur the most damage to reputation and financial penalty.

- **Integrity:** Ensures that data is accurate and unchanged from the intended source state.
- **Availability:** Ensures that the information is readily accessible to all authorised viewers, at all times.

5. ICT Services therefore deploys a range of security measures to support information security and provide for digital and physical asset protection. The approach is to focus on 3 key areas:
    - Security policies, guidance and governance arrangements
    - Security infrastructure and asset protection
    - Security monitoring

Security policies, guidance and governance arrangements

6. A range of ICT policies and guidance is made available to users so that they maximise the benefits from using technology whilst minimising the risks. Policy and guidance is comprehensive and includes the safe use of the web and e-mail, adopting complex passwords, appropriate use of mobile devices and removable media, top security tips and protecting confidential information. Policy and guidance is published on the intranet and is regularly updated and communicated to users.

7. ICT Services has many ongoing technology projects and programmes that update current software and hardware solutions and introduce new ones. The security of information and devices is considered at the design stage of all of these solutions by specialist Technical Architects and is scrutinised by governance boards prior to being introduced into the live environment.

Security infrastructure and asset protection

8. A constantly evolving threat landscape requires a multi-levelled defence strategy. With increased reliance on internet communications and connectivity, the County Council cannot rely on internal defences alone and so operates a “defence in depth” security model which offers significant protection from a multitude of cyber-attack vectors. It is the combination and interactivity of a range of products that maximise protection from internet borne threats, a brief outline of which is provided below:

    i. **E-mail filtering:** The filter inspects all incoming e-mail from external sources with the aim of delivering only clean e-mail from legitimate sources, and blocking suspicious or unsolicited messages. This includes SPAM (unsolicited junk e-mail) and phishing (fraudulent e-mails purporting to be from reputable sources) threats. The filter is a good example of a complex service/security balance as a strict filtering policy may block legitimate e-mail, and a lax policy will allow high volumes of unwanted mail.

    ii. **Device protection:** Sophos software is configured and deployed to ensure maximum protection for user devices with features including anti-virus, anti-malware, applications control and web protection. Currently all user hardware receives a full “scheduled” anti-virus scan twice a day and receive “on access” file scans throughout the working day. As an indication of the effectiveness of Sophos software, 1,497 viruses were blocked and cleaned from a single USB device connected to our ICT

network last year. Mobile devices are configured for security and encryption in line with National Cyber Security Centre best practice guidance.

iii. **Firewall:** The firewall solution is configured to control all inbound traffic to the ICT network and blocks unprompted executable file downloads, provides an additional layer of anti-virus protection, manages the internet access through web filtering policies, controls files access, highlights network risks and provides information regarding potential threats.

iv. **Enhanced firewall protection:** A solution (Palo Alto Wildfire) is used to provide an enhanced level of network security by providing real time analysis of network activity and file access, and offers significant protection from zero day threats (a software vulnerability for which there is no current fix) with protection provided within 15 minutes of an international discovery of a new variant. The intrusion detection and prevention features of this solution enable the blocking of attempted network attacks.

v. **Data sharing solutions:** The County Council uses a range of secure solutions for secure e-mail (GoPortal) and file sharing with partners (Office 365, Cryptshare).

vi. **Data backups:** The usual recovery from a successful cyber-attack is to restore data from backups. A regular routine is used for the backup of all data and much of this is held across two data centres.

vii. **Remote access:** there are a number of ways that users can currently access applications and information when away from the base using their own or County Council devices. In order to provide enhanced levels of security, and better value for money, these are being rationalised so that only County Council devices are used (laptops, tablets and smartphones) alongside our secure remote access solution (*Cisco VPN*) with legacy solutions being withdrawn (*OLVI, GetConnected* and *ADSL homeworking*).

Security monitoring

9. As part of its role in managing and monitoring the ICT estate, ICT Services uses software to identify application and operating system vulnerabilities and to highlight missing security updates, patches and legacy software installations. Remote updates can then be deployed to fix these security vulnerabilities.

10. The County Council has a secure broadband connection into the Public Service Network (PSN) that enables users to send and receive sensitive and confidential data between other public sector organisations. To connect into this secure network there is an annual independent compliance audit and assessment as to the integrity and security of the County Council's ICT network and infrastructure. This exercise not only ensures that the ICT network complies with current security standards but also identifies any low and medium level risks that need to be addressed.

11. The ICT Security Team (there are 3 security specialists) manage an e-mail account for users to report SPAM and suspicious messages. This has proved extremely useful in identifying zero day attacks as we can liaise with our providers (Sophos and Palo Alto) to provide

network protection within as little as 15 minutes, and receive a solution to remove any infection within hours.

Ongoing risks

12. The largest perceived threat of a cyber-attack on County Council services is currently via the internet and e-mail service. Whilst there is a high level of protection and multiple platforms to mitigate the risk of infection once a threat has been delivered, it is the point of entry and user behaviour that is the biggest risk.

13. The specific cyber-attack most prevalent through e-mail currently is *Ransomware*. This is a threat with the purpose of holding businesses to ransom by maliciously encrypting their data and charging a fee to allow access to the information. A typical *Ransomware* attack will initiate via an e-mail with an infected attachment. The e-mail will be worded to social engineer the recipient to open the attachment e.g. “please find attached an invoice that is overdue for payment”. Opening the attachment will execute the attack. Lincolnshire County Council were subjected to a successful *Ransomware* attack in 2016 resulting in a total loss of ICT services for a week.

14. The County Council’s ICT Strategy 2014-17 sets out the technology direction of travel and the key work programmes supporting its delivery. This includes the transition away from owning and operating a data centre and all of the associated infrastructure (servers, storage, switches, racking, power, air conditioning etc.) with a move to using off-site data centres, commonly referred to as *cloud* services. Whilst there are a range of security risks associated with this approach, they are well understood and we have experience through our current use of a second data centre at Derby. The leading technology market analysts (Gartner) advise *cloud* solutions as providing the public sector with the best security levels over the next 2 years.

15. The establishment of alternate service delivery models such as ViaEM, Inspire and ARC provides a new risk in the short term, whilst arrangements are made to segment applications and data access between the new client and contractor functions. There is ongoing activity to achieve this separation.

Reason for Recommendation

16. To raise awareness of the approach to cyber security within the County Council.

Statutory and Policy Implications

17. This report has been compiled after consideration of implications in respect of finance, equal opportunities, human resources, crime and disorder, human rights, the safeguarding of children, sustainability and the environment and those using the service and where such implications are material they are described below. Appropriate consultation has been undertaken and advice sought on these issues as required.

RECOMMENDATION

1) It is recommended that the content of this report is noted.

Ivor Nicholson
Service Director – ICT

For any enquiries about this report please contact: Ivor Nicholson on 0115 9774006

Constitutional Comments:

18. This report is for noting only so no constitutional comments are required.

Financial Comments

19. No financial comments required.

Background Papers

- None

Electoral Division(s) and Member(s) Affected

- All