ESSEX FIRE AUTHORITY

Essex County Fire & Rescue Service

MEETING	**Audit Governance & Review Committee**	AGENDA ITEM	**10**
MEETING DATE	13 July 2016	REPORT NUMBER	**EFA/095/16**
SUBJECT	**Cyber Security**		
REPORT BY	Finance Director & Treasurer, Mike Clayton		
PRESENTED BY	Finance Director & Treasurer, Mike Clayton		

SUMMARY

This report is designed to demonstrate to the Committee the arrangements in place within the Authority for the management of cyber security and information security.

RECOMMENDATIONS

Members are asked to review and comment on the arrangements in place.

BACKGROUND

The issue of cyber security has gained a higher profile following recent successful impactful attacks on local authorities, in particular Lincolnshire County Council[1]. Whilst the Authority faces a level of sustained continual attack, it was also recently the subject of a more sophisticated email-borne attack which successfully evaded some of the Authority's technical controls. In this case, the vigilance of some Authority employees alerted us to the threat, which enabled added control measures to be put in place until the technical controls were updated by the vendors.

Cyber risk is included on the Authority's corporate risk register with the controls are in place to protect the Authority from the risk. In addition the Authority exchanges information with the government CESG Group (Part of GCHQ) to ensure that we understand the latest risks. The sections within this paper follow the GCHQ document "10 Steps to cyber security"[2] and outline the Authority's internal assessment of position against each of the 10 measures.

Within the ICT team the Authority employs a dedicated ICT Security Officer to oversee and operate control measures and perform risk assessments for projects and other changes. Many staff within the ICT department carry out duties that underpin the defences against the cyber threat. The ICT resources are collectively engaged, in a stretched capacity, in delivering the

[1] http://www.bbc.co.uk/news/uk-england-lincolnshire-35453801

[2] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Authority's ICT changes (e.g. Delta / MIS replacement). However, it is also important to understand that an effective defence against the cyber threat relies upon the entire organisation being well-informed and alert to the continually evolving attacks. This isn't solely an ICT issue.

The Senior Information Risk Owner for the Authority is the Finance Director & Treasurer who receives regular briefings from the ICT Security Officer and external sources.

A key part of the Authority's ICT strategy is to shift services to 'the cloud', using highly capable and mature organisations such as Microsoft. This shift is viewed as a security enabler, allowing the Authority's ICT team to more effectively focus its resources on those components that can only be delivered locally.

REDUCING THE CYBER RISK IN 10 CRITICAL AREAS[3]

The section below looks at the 10 areas identified by the government as critical to the management of the cyber risk. The current status of these controls has been RAG assessed and they will be managed through the Service's risk management tool.

INFORMATION RISK MANAGEMENT REGIME (STATUS: AMBER)

In 2015, the Authority recognised the benefits of having an Information Security Management System (ISMS) and embarked upon an ISO27001:2013 implementation. However, this activity was subsequently stopped due to there being insufficient capacity to proceed with other high profile projects and organisational change activities taking precedent. In the meantime, the ICT Security Officer is implementing ISMS best practices in a tactical manner. Whilst this approach is closing gaps, it takes significantly more time and effort to make progress.

SECURE CONFIGURATION (STATUS: AMBER)

Mobile and desktop devices are secured by the ICT department to prevent users from adding applications that can interface with Authority systems. Systems are patched and proactive scanning takes place to maintain awareness of technical vulnerabilities. Improvement opportunities exist in patching and looking to disable the ability to access removable media (e.g. USB memory sticks).

NETWORK SECURITY (STATUS: AMBER)

Multiple layers of defences are in place to protect the service from attack from untrusted networks (e.g. Internet), including Firewalls and Web/Email gateways. Improvement opportunities remain in network security and making better use of the real-time threat detection capabilities.

MANAGING USER PRIVILEGES (STATUS: AMBER)

The Authority has implemented a least-privilege access model, to grant users the minimum level of access required to carry out their role across all ICT systems. ICT grant network and business system access upon receipt of authorisation, with audit trails in place. There are improvement opportunities in reviewing and removing business system access and in having improved awareness of non-employees (e.g. contractors, suppliers).

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

USER EDUCATION AND AWARENESS (STATUS: AMBER)

The ICT Security Officer used recent detected attacks (e.g. phishing[4]) and other information security incidents (e.g. information loss) to promote wider awareness of the risks to the Authority. Further pro-active messaging will be used at regular intervals to maintain awareness. Evidence from a recent phishing attack suggests that the majority of Authority employees are aware of the risks and do not open suspicious emails. There are improvement opportunities in establishing a more formal information security training programme and ongoing compliance based awareness.

INCIDENT MANAGEMENT (STATUS: AMBER)

There is a documented policy for reporting of all cases where cyber or information security may have been breached, included physical breaches or thefts. The policy provides for the notification of the incident and the internal investigation. As a result of this approach one loss of personal data was investigated and reported to the Information Commissioner's Office in the first quarter of 2016. There were no such instances in 2015. Improvement opportunities needed to establish more formal incident management protocols for the event that the Authority was to sustain a chronic successful cyber-attack.

MALWARE PROTECTION (STATUS: GREEN)

The Authority employs layers of defence against the malware threat. The majority of malicious content received from untrusted networks (e.g. the Internet) is successfully filtered out before it reaches the end users. PCs and Servers are protected with a managed anti-malware solution and malware detection is routinely followed up on. End users do not have "administrator" permissions on their PCs, which limits how some threats are deployed. Also, the Authority uses virtual desktop PCs which are rebuilt every night (along with any malware that could be deployed). Defences in place are also in place to stop successfully deployed malware being able to "call home". Improvement opportunities are in implementing ongoing anti-malware scanning on certain platforms.

MONITORING (STATUS: AMBER)

Monitoring of the logs of critical assets is in place and used to support post-incident follow up. However, this is complex and resource intensive area and much improvement is needed to make better and more proactive use of this information. The Authority's monitoring platform is up for renewal in 2016, with an alternate deployment method being favoured (e.g. platform or service outsource).

REMOVABLE MEDIA CONTROLS (STATUS: AMBER)

Removable media, such a memory sticks are required to be encrypted and password protected before they can be used to store Authority information. This mitigates the risk of information loss if the removable media is lost or stolen. Scanning of removable media is performed, to minimise the risk of introducing malware to the environment. Improvement opportunities exist to review the need for Authority employees to have access to removable media at all (i.e. adopt an access by exception approach).

[4] Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

HOME AND MOBILE WORKING (STATUS: AMBER)

The risk of remote working is primarily managed through deploying a secure gateway which uses two-factor authentication (i.e. network password and a security token) to ensure the person accessing the system is the person authorised to do so. Laptops are protected by full disk encryption. Authority data on tablet devices is held in a secure area that can be deleted if the device is reported as lost or stolen. A change of approach is currently being introduced for tablets, to manage/control the entire device (i.e. view it as a corporate-owned asset). Improvement opportunities in defining a more formal policy and training for this specific use case and maintain a formal ongoing security awareness programme.

RISK MANAGEMENT IMPLICATIONS

The controls listed in the paper are the main controls used to manage the risk of a breach of cyber security preventing the Authority providing a service to our communities. There are additional business continuity controls that also help to mitigate the impact of this risk.

Dealing with the cyber security threat is something requires strong participation across the organisation, in particular with Internal Communications, Property, HR and Training, and ICT.

OTHER IMPLICATIONS

There are no other legal, financial, health and safety, equality or environmental implications from this report.

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985	
List of appendices attached to this paper:	
Proper Officer:	Mike Clayton
Contact Officer:	The Finance Director and Treasurer Essex County Fire & Rescue Service, Kelvedon Park, London Road, Rivenhall, Witham CM8 3HB Tel: 01376 576000 mike.clayton@essex-fire.gov.uk :