Cyber Security

This document is in response to correspondence from Cabinet Office regarding Cyber and Ransomware following successful attacks on Local Authority targets. I have taken each element contained in the Cabinet Office letter relating to back-up, cyber security and ransomware and detailed our current position and what action we would like to take.

Staffing

We currently have a vacancy in the team for a Support Analyst. We were retaining this post for the CRM implementation/support but because we have procured Netcall Liberty low code that post has been picked up by other team members. Cyber security is so essential to the protection of our IT environment and ultimately the ability of the authority to operate that we would like to use this post for an analyst focussed on Cyber Security.

Backups

Are we backing up the right data?

We currently backup all databases, virtual servers, production datastores and development datastores where required.

Are the backups are held offline?

We backup to on premise and cloud backup (CT Cloud backup) that is not on our network.

The CT Cloud backup includes Insider protection which is an air gap to prevent data loss from an internal bad actor. CT Cloud backup also includes our entire Office 365 environment as despite popular myth, you do need a separate backup of your Office 365 environment.

https://www.ct.co.uk/cloud/secure-cloud-backup

Have we tested that we can recover data and services from backups?

We have restored several backups of Live databases into the test environment for ongoing upgrade and testing work. We have carried out several Mailbox restores and recovery of Sharepoint documents and folders.

Annex items

Ransomware

We are currently reliant on perimeter defences to protect against Ransomware(firewall, mail filter, AV). Although these do provide some protection, it is clear that a successful Ransomware attack is more of an inevitability than a probability. We need to implement further protection to stop an attack before we are held to ransom.

We are currently assessing two Cyber Security products, Cyglass and Bullwall RansomCare.
Cyglass – this product is network intrusion detection software and gives visibility of our network traffic and identifies traffic that may be suspect. (heuristics of known threats). We are currently running this product as a proof of concept as the supplier wants to establish a UK Local Authority market.
RansomCare – this product is for the monitoring and containment of Ransomware. It looks for any encryption activity on the network or Sharepoint online and stops it. We have a quote for the implementation of this product for £2,500 per quarter. We would like to procure and implement this immediately.

Phishing guidance.

We have implemented a Mimecast tool that prevents impersonation emails from being sent into the organisation from email addresses with Management Board display names. Mimecast also includes the external email warning. We are considering extension of the impersonation tool to Councillors and SMT.

The NCSC Early Warning Service

We are signed up to the NCSC Early Warning Service and it identified 3 issues so far that we have resolved. It emails us of potential issues.

Protective Domain Name Service

We have implemented the Protective Domain Name Service that checks web traffic going out of the Waverley domain against known malicious domains and will not resolve to that address. We receive a daily update and monthly summary that shows blocked traffic. A secondary product, Roaming Domain Name Service for corporate laptops is to be investigated.

Web Check

We are signed up to the Web Check service and it is checking all our public facing websites

Mail Check

We have implemented the NCSC Mailcheck using DMARC, DKIM and TLS configuration.

Logging Made Easy

We are going to implement Logging Made Easy and Jamie is attending some training on this solution.

Exercise in a Box

This service allows an organisation to find out how prepared it is for a cyber attack and to improve planned response. This is something a cyber analyst could take forward for us.

Test Phishing email

We would like to carry out some test phishing activity to educate staff. This would simulate phishing emails into the authority and collect information on staff who react.

Training

We should repeat the training from South East Regional Organised Crime Unit and make it compulsory. This trains the end users in what to look for in both Corporate and Personal environment.