Paper for: The Finance and Audit Committee

Title: Agenda Item 9 - Cyber Security

Date: 14th September 2021

Strategic Purpose: Risk Management

Resource Implications: Financial for adequate IT infrastructure and management

F&A Committee: To review the risks and mitigation measures

Introduction

In September 2020 the committee received a paper setting out the cyber security risks and mitigations operated by the LEP (and, as we share a common platform, Marketing Cheshire).

At that time staff had essentially been working 100% from home for a few months and we had little concept that a year later the situation would largely remain the same. Continuing to function as an organisation has been critically dependent on IT and digital technologies. Information is created, acquired, stored and re-used on a daily basis and should those systems fail or be infiltrated by malicious operators, considerable damage to the LEP would result.

While the LEP maintains a significant information resource, as last year, the vast majority of it would be classified as "Official" within the context of Public Sector information. Occasionally some data sets, e.g. those which contain a significant amount of personal information, will require additional protection and very occasionally we are in possession of commercially sensitive information. However, none of the information held by the LEP would normally be classified as "Secret" or above, and the measures we take are therefore proportionate to the categories of information held.

The Threat

The shift to digital working adapting to the pandemic has been accompanied by an increased threat from malicious actors, seeking to profit or disrupt. An article in the MJ earlier in the year estimated that Local Authorities had experienced an increase of over 200% in malicious traffic.

What has been noticeable over the past year is an increased number of system patches and updates being applied by our third-party IT service provider and other infrastructure providers. This work tends to be performed outside of normal business hours, so users experience little disruption to services. However, as the main point of contact for notification, there has been a sharp rise in maintenance and while some relate to infrastructure to manage the new demand levels, others are patches to e.g., firewalls etc.

Also, as a reminder, the committee was informed at its June meeting that the LEP Growth Hub website had been compromised and was distributing unsolicited advertising material. Our response was to shut it down because we were already on the verge of launching a new website and the impacts were relatively minor. However, it could have been different and we learned of the risks posed by web developers accessing plug-in source code as a short cut to providing functionality which is, then, subsequently not maintained sufficiently well.

Cyber Risks and Management

As in the past, we set out to follow the framework laid out by the National Cyber Security Centre and the requirements of Cyber Essentials. While the LEP does not seek accreditation, this framework provides helpful guidelines and specifies requirements under five technical control themes:

• firewalls

• secure configuration

• user access control

• malware protection

• patch management

Appendix 1 sets out in more detail how we address each of those topics and is a repeat of what we said last year.

Devices

LEP employees are provided with IT devices and mobile phones by the company configured for use with the organisation's IT systems. Bring your own devices is not generally needed or sanctioned but that is not to say that some staff will be able to access some services, e.g. their email and Office 365 account, via a personal device. The "economy" in Marketing Cheshire is more mixed; personal mobile phones are used more frequently. And contractors are often required to use their own equipment to avoid being deemed an employee for HMRC purposes.

The LEP operates IT Use policies which restrict personal use of IT devices and inappropriate websites.

Social Engineering

While it is relatively straight forward and effective to mitigate risks by installing various hardware and software measures, the greatest risk to infiltration of the system is by a user being "tricked" into opening a document or to perform an action, such as making a payment, by what they believe is a genuine email. As a transparent organisation with names and details of our staff on the website, it is quite possible for bogus emails to be created purportedly from, e.g., Philip Cox to a member of staff asking for a payment to be made or to click on a link.

Our first step in mitigating this risk is regular reminders to staff to be vigilant, which we do from time to time at weekly all staff team meetings, and to be on their guard for something that at first glance might appear genuine and to query any item about which they hold suspicions. We support that by some additional training exercises to raise awareness and knowledge.

As an additional check we occasionally perform a sweep of the dark web to identify whether LEP email addresses and, more importantly, passwords appear. Should we discover anything of significance individual members of staff will be approached and instructed to change passwords.

Ian Brooks

September 2021

Appendix 1

Summary of Controls

Firewalls (Perimeter Security)

Protecting the edge of the network is vital to Cyber Security strategy. The LEP have invested in both the threat protection technology and outsourced security business to help protect both the employees and assets within the LEP IT environment.

UTM (Unified threat management) is used on the firewalls to provide a host of protection technology including;

1. Antivirus
2. Content Filtering
3. Application Control
4. Intrusion Prevention Services. (IPS)
5. Sandboxing (a separate environment to test applications so they cannot harm the underlying operating system).

Although the equipment and licensing are in place there is a requirement for specialists to over-see the systems in place. To achieve this continual review a SOC (Security operation centre) is required to protect both the LEP assets and people. The LEP outsource security of the firewall to Blaze networks who layer additional services onto the above security hardware including;

1. Change control
2. External vulnerability scanning
3. Sys logging
4. SIEM (Security Information and Event Management)

Secure Configuration

Maintaining secure configuration is one of the largest challenges in today's IT environment. Computers need to be kept up to date with security updates, new equipment needs bad configurations removing and known security configurations implementing. Below are the measures the LEP has in place or are services used from Blaze networks to maintain a secure configuration within the LEP.

- Blaze provide Remote monitoring and management (RMM) services as part of their IT services support provision. This capability allows Blaze to implement patches and software updates to ensure all systems are kept up to date within the LEP.
- Internal vulnerability scans are run to confirm and ensure all internal systems are in a secure state.
- All manufacturer defaults are removed from equipment before being installed.
- Only systems provided from Blaze are installed in the network. Blaze build each system from a trusted image. That image is then used on systems before they are deployed in the LEP.
- Separation of areas within the network are provided. For example, corporate and guest wireless access are completely separated. In addition, voice traffic operates on its own independent virtual local area network (VLAN).

- Microsoft 365 is used to provide data service including email, sharepoint, teams etc. All Microsoft services are protected with two factor authentication (Password and PIN sent to a separate device).
    - Multiple layers of separation have been provided in the file systems so data access is provided on a needs only basis.
    - Email provides both encryption via transport layer security as well as Anti-Spam and Antivirus services provided through Blazescreen Email.
- All business mobile phones and laptops are encrypted using mobile device management software (MDM). In addition to encryption the MDM cloud driven application allows Blaze to lock or remote wipe laptops and phones in the event they laptop or phone is lost or stolen.

User Access Control

User access can be compromised if relevant measures and a good framework / procedure is not in place. The LEP has an outsourced IT service functions to a managed security services provider MSSP. By doing this, a number of challenges are addressed both from a systems level and service level.

Type of controls and procedure in place include;

- Password – renewed every 90 Days.
- Full logging retained at a server level.
- Enforced Password Complexity.
- Single identity source for all authentications.
- User template forms for new starters and leavers and an onboarding process.
- Two factor authentications for Microsoft 365 services.
- Two factor authentications for VPN services.
- Enforced Phone Pin protection through MDM.
- Microsoft 365 document security.

Malware Protection

Malware protection is a basic level of mitigation against inbound threats. Best practices dictate multiple levels of protection. Blaze provide the following protection as internet traffic enters the network.

Fortinet Unified threat management (UTM) including IPS, AV, content filtering, application control, sandboxing.

When internet traffic has passed the perimeter network there is then a final level of security provided on the desktop machine.

This protection is provided through bit defender and provides antivirus, intrusion prevention, and application control.

Patch Management

It is vital to close known security vulnerabilities by maintaining a vigorous patch management schedule. The LEP outsource the management of network devices to Blaze Networks who provide the following levels of patch management.

- Laptop and Desktop operating systems – Are patched on an automated schedule each week through the Blaze Network RMM service.
- Core firewalls are upgraded on a specific track supported by Blaze the managed security service provider (MSSP). Threat management updates are sent daily or in real time and feature updates are provided monthly or quarterly.
- Core switches and Wireless are also updated on a quarterly basis.
- Phone systems and IP phone are updated each year.