Basic cyber security questions for your IT Advisors

For many law firms, dealing with cyber prevention can be mind boggling in its complexity. 'Attack surfaces', 'threat actors', 'dark web' – all the associated terms strike fear into the heart and often lead either to expensive knee jerk reactions or the proverbial 'head in the sand'.

My intention is not to down-play the seriousness of a cyber-attack and the fallout from it (I have assisted firms in recovering from these events so am acutely aware of how serious it can be) but to offer simple advice that will give you confidence in your conversations with suppliers and a level of comfort that you have tackled the basics.

With the predominance of Microsoft 365, I thought I would cover this in the first in this series of articles.

365 is a suite of products all of which are controlled from an online 'Admin Centre' portal. Your IT Team or Service Provider will have access to this, but often we have found that these "administrators" see their role just as the keepers of your licensing – they add and remove users. Managing cyber security related settings may not be part of your agreement with your MSP.

Within the admin portal there is a huge range of security related settings. When your Microsoft business account (known as a 'Microsoft tenant') is created, most of these settings default to 'Off' and it is your responsibility to switch them on.

Note: Sadly, it is also often the case that MSPs don't know enough about the depth of functionality available within MS365 or keep on top of changes. Most see M365 as a "point in time" solution which is configured once and left well alone.

However, MS365 is not a traditional product with Microsoft making and rolling out thousands of changes each year. To get the best out of MS365 and the security it provides it needs to be proactively managed. In short, if you are using an outsourced MSP do not assume they have done all of this for you – hence the need to ask the questions both of MSPs and internal IT teams.

Here are the key features, with some questions that you could put to your IT Team/MSP:-

1. **Identity and access management:**

    a. **Multi-factor authentication (known as MFA or 2FA)**

A code will be sent to the user's phone as they log in (both periodically and when they log in from a different location or device). Some firms don't apply this as they are concerned that staff will get fed up with constant notifications. Rest assured they don't have to be that frequent and they aren't that bothersome. However, having MFA gives you something in the region of 85% more protection than a basic password. For this reason, it is definitely a recommended feature and a prerequisite for Cyber Essentials.

We should also note that the Cyber Essentials guidance is that all applications should be covered by MFA. For applications installed on your networks the "logon" MFA will cover this need, but solutions accessed on the internet (e.g. client onboarding portals) should also have their own MFA solution.

It is also possible to turn off MFA from trusted locations, such as your offices. Best practice is that any access remotely from your controlled network should require MFA.

Ask your IT Team/Service Provider whether you have MFA switched on for ALL cloud-based services, including MS365, as well as access to your own network.

b. **Conditional access policies**

These policies are 'if / then' statements that govern access to all or part of your system. I.e. if the user has permissions, they can access company confidential folders, if the user is not in the UK don't let them log in, etc.

One of the key components is the geographical location – you can tweak this for those that do work abroad, but generally speaking you will want to be alerted if someone logs in from another country unexpectedly, or where there are other 'risky' sign in conditions.

There are certain countries that are higher risk, and it is recommended that access from these countries is denied, but best practice is that you block access for all locations other than those your business operates from. This will mean access from outside of those locations will need to be planned in advanced for those who travel.

Ask your IT Team/Service Provider whether the 'location condition' has been switched on in MS365 Conditional Access Policies.

There are a number of conditional access policies that are available if you are on the 'Business Premium' or 'Azure AD Premium' license for MS365. This gives you access to a product called InTune (used to manage your devices connected to your Microsoft business account, such as laptops, desktop PCs and phones). Once you have this, you can lock down access only to devices that have been registered to you and meet certain criteria.

For example, it is important that any device accessing your systems has the latest updates and patches from a provider such as Microsoft. These will contain security updates, so are critical. InTune can be used to enforce this and can refuse access to your systems if the required updates and patches are missing.

Ask your IT Team/Service Provider what version of MS365 licensing you have, whether it includes InTune and, if so, whether InTune has been set up and all devices enrolled.

c. **Role-based access control**

This feature allows you to give permissions to people either individually or by creating groups to which individuals are assigned. The key security point here is that a system administrator should always have two accounts – one for administration and one for normal day-to-day work. The reason for this is that if an administrator has one account that has wide access across your systems, and they are using this also for emails, browsing and other normal activities, they are therefore exposing a wide area of your data to all of the risks that come with access to the outside world.

Ask your IT Team/Service Provider whether administrators all have separate accounts from their normal day-to-day accounts (and whether they are covered by MFA, see above).

2. **Threat protection**

Microsoft Defender is included with 365 Premium Business licenses and includes a range of features, such as anti-virus and anti-spam filtering, advanced threat analytics, and behavioural monitoring. It can be run alongside most other anti-virus software.

Ask your IT Team/Service Provider whether Microsoft Defender is switched on and whether it has been deployed with all of the default settings or configured for the business.

If not configured for your business, you may want to ask your provider to talk you through the options.

3. **Compliance management**

Known as 'Purview', the Microsoft 365 Compliance Portal includes tools to help organisations meet their regulatory compliance requirements, such as GDPR and ISO 27001. This only applies to data in MS365 – emails if you are in Exchange online, documents and data stored within Sharepoint and/or OneDrive and data and documents in Azure.

Ask your IT Team/Service Provider whether the Microsoft 365 Compliance Portal has been configured for your business and whether all of your data and documents are in scope of that Portal.

Purview allows you to set up policies to govern data, manage devices and receive alerts. Once configured, you can catalogue your data, audit it, do content searching, data investigations, eDiscovery, data subject requests, etc. You can then go on to set up Data Loss Protection (see below) and deliver data back to the business about your compliance and information governance.

A good example of this is you can identify emails which contain bank account / credit card details and manage them differently to "normal" emails.

4. **Data loss prevention**

Microsoft 365 includes data loss prevention (DLP) features that allow administrators to create policies to prevent the sharing of sensitive information with the wrong people either inside or outside of your firm.

Much of the DLP feature set is derived from properly implementing Purview (above) – you won't know how important your data is until you have catalogued it, classified it and created policies to govern what you can do with it. MS365 then layers on certain software that applies policies as that data moves around or outside of your firm.

For example, Microsoft Exchange will look for sensitive information in emails and apply those policies.

Ask your IT Team/Service Provider firstly whether the Microsoft 365 Compliance Portal has been configured (as above), and then where those data governance policies will be applied.

5. **Secure collaboration**

MS365 comes with products such as Teams and Sharepoint, which allow users to share documents or folders internally and externally. By default, there are no limits on sharing and no limits on the number of Teams channels or Sharepoint folders that users can create.

This is a significant risk – mistakes can be made in sharing with the wrong people, forgetting who you have created shares for, not removing shares at the appropriate time, etc.

From the admin portal and Sharepoint features of MS365 you can disable sharing entirely, limit it to individuals or group, limit what the recipient can do (i.e. view the shared files only) and you can monitor the shares that are in place.

Ask your IT Team/Service Provider whether there are any limitations currently in place on sharing Teams channels and Sharepoint folders, and whether it is being monitored. If not, ask them to advise on setting this up.

6. **Audit and reporting**

Most of the products and activities in Microsoft 365 have audit logs capable of recording each activity. In the event of an incident (being that a technical issue, internal governance issue or cyber event) these logs can be crucial.

These logs are turned on by default but can be switched off. The default retention for these logs is 90 days but they can be retained for up to a year (depending on licensing). Purview (mentioned above) is used to configure these logs and search them.

Ask your IT Team/Service Provider to confirm that MS365 auditing is switched on, and for how long the audit log is kept.

Hopefully, this article will provide you with enough questions to get a good understanding of the way MS365 is (or can) secure your business, if configured properly.

Note that this is only one element of securing your systems (more articles to follow), and you can't guarantee that your IT providers have made the changes in the best way, so it is important to consider engaging security experts or at least garnering a second opinion.

If you take two things from this article, please let them be that 1) just because you "have" MS365 it doesn't mean you are secure, and 2) don't assume your IT provider is fully au fait with all elements of MS365 and how to best secure you.

Please get in touch if you need more information or the answers you get from your IT advisor aren't giving you confidence that your MS365 environment is secure.

Cathy Kirby, Baskerville Drummond