**Considerations for the Legal Sector**

[Asset Register and audit 1](#_Toc118894100)

[Reviewing passwords and 2FA 3](#_Toc118894101)

[Phishing 3](#_Toc118894102)

[Reviewing Firewalls 4](#_Toc118894103)

[Backups 5](#_Toc118894104)

[Secure Configuration 5](#_Toc118894105)

[Security Update Management 5](#_Toc118894106)

[Malware Protection 6](#_Toc118894107)

[User Access Controls 6](#_Toc118894108)

[BYOD and IOT 6](#_Toc118894109)

[Accreditation 7](#_Toc118894110)

#

# Asset Register and audit

Although best practice would be to carry out regular reviews of the devices and programmes that you are using, this is not always practical. So, an annual review is the very least you should pencil in.

## Why do I need one?

Unless you know what assets you have, you can’t make any decisions about the risk those assets pose. If an alert comes out about a particular product you can review your list, knowing that it is comprehensive, and be confident about whether you need to act or not.

## What should it include?

* **Hardware** – e.g., laptops, servers, printers, but also mobile phones or USB memory sticks.
* **Software** – not only the purchased software, but also freeware.
* **Information** – not only in electronic media (databases, files in PDF, Word, Excel, and other formats), but also in paper and other forms.
* **Infrastructure** – e.g., offices, electricity, air conditioning – because those assets can cause lack of availability of information.
* **People** - People are also considered assets because they also have lots of information in their heads, which is very often not available in other forms.
* **Outsourced services** – e.g., legal services or cleaning services, but also online services like Dropbox or Gmail – it is true that these are not assets in the pure sense of the word, but such services need to be controlled very similarly to assets, so they are very often included in the asset management.

The expected details within the register include:

* **Name:** A simple and clear label – bear in mind this label might exist across any number of documents.
* **Description:** Consider what the asset does and how it enables business.
* **Location**: Where is it stored, hosted, and maintained?
* **Owner:** Who, at a senior level in the business, most benefits from the asset?
* **Users:** The business units and personnel who use the asset.
* **Classification & Caveat**: Official, Official-Sensitive, Secret, Top Secret etc.
* **Size:** Number of records, data subjects, case files etc.
* **Personal data**: Yes or No.
* **Format**: Database records, spreadsheets, word documents, paper files etc.
* **Risks**: Considerations of the loss of Confidentiality, Integrity, or Availability of the asset.
* **Key Asset**: Yes or No – i.e., how important is this to your business

Once you have an asset register you can consider the risks to your organisation and using this understand what systems and data required greater protection than others.

You need to list all your assets, then threats and vulnerabilities related to those assets, assess the impact and likelihood for each combination of assets/threats/vulnerabilities and finally calculate the level of risk.

If you do spend the time to have the comprehensive asset register and a clear knowledge of the risks, to you will be able to understand what data you have, where it is held, but more importantly what systems and data are essential of the running of your company. When you understand this then you can focus efforts to ensure that this is the most protected and potentially the first to be recovered if a cyber incident does occur.

## Working out your risk

Threat x Vulnerabilities x Impact x Likelihood = Risk

|  |  |
| --- | --- |
|  | Impact |
| **Insignificant** | **Minor**  | **Moderate** | **Significant** | **Catastrophic** |
| Likelihood | **Probably** | Low Med | Medium | Med Hi | High | High |
| **Possible** | Low | Low Med | Medium | Med Hi | High |
| **Unlikely** | Low | Low Med | Medium | Med Hi | Med Hi |
| **Rare** | Low | Low Med | Low Med | Medium | Med Hi |
| **Negligible** | Low | Low | Low Med | Medium | Medium |

## What will you do about the risk?

1. Reduce the risk - apply security controls decrease the risks – using a framework can help in this area such as cyber essentials or ISO27001. This could be acknowledging that you have an obsolete system which should be retired but is essential, so you put immediate plans in place to ringfence it away from the internet so it’s not compromising your entire system and then have a plan to replace it as soon as possible.
2. Transfer the risk to another party – e.g., to an insurance company by buying an insurance policy.
3. Avoid the risk by stopping an activity that is too risky, or by doing it in a completely different fashion. This might be recognising you have an obsolete system and replacing it straightaway with one which is support and not vulnerable to criminals.
4. Accept the risk – if, for instance, the cost for mitigating that risk would be higher that the damage itself.

But unless you know the risk then you can’t take any of these actions – you’re just ignoring it. If you then have a data breach and the ICO asks how you managed the risks within your company, you won’t be able to give any rationale for the policies and procedures you have.

# Reviewing passwords and 2FA

|  |  |
| --- | --- |
| **Have you…** | **Yes or No** |
| Reviewed your own email and telephone number on [www.haveibeenpwned.org](http://www.haveibeenpwned.org) within the last 6 months (both personal and work accounts)? |  |
| Shared www.haveibeenpwned.org with staff, family and friends? |  |
| Registered your company’s domain on [www.haveibeenpwned.org](http://www.haveibeenpwned.org) so you can receive notification if your domain appears in a data breach? |  |
| Ensured your staff know what a strong/weak password is? |  |
| Stopped re-using passwords and ensured your staff are not? |  |
| Generated strong password using the NCSC’s three random words (e.g. Storm22Generated##Runaway)? |  |
| Enabled use of password manager for self and staff? |  |
| Enabled 2FA on yours and your staff’s email accounts? |  |
| Ensured all company social media accounts have 2FA enabled? |  |
| Ensured 2FA is set up on any other essential software/system? |  |
| Ensure accounts lock after no more than 10 unsuccessful attempts to defend against a [brute force attack](http://www.ecrcentre.co.uk/glossary#comp-kob6g2wa) |  |
| Carry out regular checks of physical hardware for [keylogger USBs](http://www.ecrcentre.co.uk/glossary#comp-kob6keo8) |  |
| Changed all default passwords wherever you find them |  |

# Phishing

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Employed anti-spoofing controls so that attackers can’t pretend to be you, namely [DMARC, SPF, DKIM](https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing)? |  |
| Checked your email security settings are correct with NCSC’s free tool - [Email Security Check](https://emailsecuritycheck.service.ncsc.gov.uk/)? |  |
| Understood what information is published that could be used to create spear phishing email – those targeted to a particular person/department with personalised content? |  |
| Filtered or blocked incoming phishing emails using your email provider or specific service? |  |
| Trained your staff to identify phishing? |  |
| Trained your staff in what to do if they receive a phish and if they act on the phish (clicked that link/opened that attachment)? |  |
| Considered using the [Outlook add-in](https://www.ncsc.gov.uk/guidance/configuring-o365-outlook-report-phishing-for-sers) to report phishing directly to the National Cyber Security centre? |  |
| Considered the technical defences such as disabling auto-run and macros or blocking specific extensions? |  |
| Used a proxy service to block any attempt to reach websites which have been identified as hosting malware or phishing campaigns? |  |
| Using a security logging system to pick up on those incidents that your users are not aware of (there’s a free one from the NCSC [Logging Made Easy (LME)](https://www.ncsc.gov.uk/information/logging-made-easy) ) ? |  |
| Got an incident plan ready and tested it for if a phishing attack succeeds? |  |

# Reviewing Firewalls

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Got a firewall(s) installed and switched on across your boundary and devices? |  |
| Ensured your firewall(s) monitors both traffic coming in to and leaving your network? |  |
| Disabled or removed any functions, accounts, or services you do not need? |  |
| Made sure that all default passwords been changed to one that is individual, unique, and secure? |  |
| Ensured the firewall updates are automatically enabled and scheduled? |  |
| Blocked unauthenticated inbound connections by default? (Inbound refers to connections coming into a specific device (host/server) from a remote location. e.g. A web browser connecting to your web server is an inbound connection (to your web server). This is sometimes known as “deny all” rule and ensures that only the traffic you have approved is allowed into your network.) |  |
| Ensured inbound firewall rules are approved and documented by an authorised individual? (This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or sub-interface on the firewall.) |  |
| Ensured your ACLs are specific to the exact source and/or destination IP addresses and port numbers whenever possible? |  |
| A plan to review rules on a regular basis to remove or disable permissive firewall rules quickly, when they are no longer needed? |  |
| Prevented access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:* + a second authentication factor, such as a one-time token
	+ an IP whitelist that limits access to a small range of trusted addresses
 |  |
| Considered whether Police CyberAlarm can provide additional useful threat reporting? |  |

# Backups

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Identified what data you need to have backed up |  |
| Kept your backup separate and offline |  |
| Considered using a cloud backup solution |  |

# Secure Configuration

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Removed and disable unnecessary user accounts (such as guest accounts and administrative accounts that will not be used)?  |  |
| Changed any default passwords and implement 2FA if enabled? |  |
| Ensured any Wi-Fi networks are password protected (and changed from default passwords)? (Consider switching SSID broadcast off) |  |
| Removed or disabled unnecessary software (including applications, system utilities and network services)? |  |
| Disabled any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the internet)? |  |
| Got a password policy in place that includes password/account lockout, re-use and resetting? |  |

# Security Update Management

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Ensured all operating systems, apps and firmware are running legitimate and licenced software? |  |
| Made sure that all operating systems, apps and firmware are regularly updated, and patches applied? |  |
| Enabled all critical or high-risk patches to be applied within 14 days of being released? |  |
| Considered legacy planning for all operating systems and software where it is known it is coming to its end of life? |  |

# Malware Protection

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Installed (and switched on) anti-malware on all computers, tablets and mobile devices? |  |
| Configured your anti-malware to: * Scan files automatically upon access?
* Scan webpages automatically when access through a web browser?
* Prevent connections to malicious websites on the internet?
 |  |
| Limited the installation of applications to an approved set (i.e., using an App Store or application whitelisting)? |  |
| Utilised applications sandboxing? (This is where you section off a program on your hard drive so that its exposure to the rest of your apps and critical systems is minimised or eliminated.) |  |

# User Access Controls

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Got a dedicated person/company looking after your IT? |  |
| If not, have you made sure that no one is running as an administrator who doesn’t need to be?  |  |
| Confirmed that they only use admin accounts for admin tasks (this might mean that one person has an admin and a user account)? |  |
| Confirmed with your outsourced IT company, that the credentials for your admin access are different from other clients (so a breach at your MSP or disgruntled employee couldn’t access all the accounts they look after)? |  |
| Ensured that the admin account is secured with Multi-Factor Authentication? |  |
| Followed the principle of least privilege for user access with an appropriate policy for reviewing and revoking of access to user accounts? |  |
| Ensured that each individual user has an individual username and password for accessing the network? |  |
| Got a policy to deal with how user accounts are set up and deleted? |  |
| Got a way to regularly review users access permissions? |  |

# BYOD and IOT

|  |  |
| --- | --- |
| **Have you…?** | **Yes / No** |
| Made a clear decision to allow Bring Your Own Devices within your company? |  |
| Got a comprehensive policy that details the expectations on your employees with regards to how they use their own devices? |  |
| Considered if Containerisation or Mobile Device Management software can be utilised for your staff’s devices? |  |
| Ensured that you have set up role-based access to systems (access to only what they need)? |  |
| Trained your staff about the risks and consequences of poor cyber hygiene and resilience, to both them and your company? |  |
| Set up a guest Wi-Fi to isolate any viruses brought in by BYOD devices? |  |
| Set up charging areas rather than having users charge via their computers? |  |
| Got a clear path to review potential IOT implementation, ensuring that the security of the device is considered at an early stage? |  |
| Changed all default passwords/ removed unnecessary accounts within your IOT devices? |  |
| Ensured that IOT devices are also subject to the principle of least privilege (access only to what it needs)? |  |
| Set up separate networks for your smart devices, so any infections or intrusions are limited? |  |
| Ensure your data is encrypted? |  |
| Ensure that you know and track the devices that are connecting to your network?  |  |

# Accreditation

There are a lot of different reasons why your company might want to get a cyber resilience accreditation, including as a requirement for a specific contract or supplier. But accreditation should be more than a tick box exercise, you should be using these as a way for you to check that the standards of your cyber resilience are adequate for the risk your company holds.

As well as ensuring that you are protect your company and your employee’s livelihoods, accreditation also has these benefits:

* **Professional reputation** - you can demonstrate to your customers that you take cyber resilience seriously. Cybercrime is increasing so being able to tell your customers that you are doing everything you can to protect them has got to be good. Can your competitors say the same?
* **Independent verification** - you may have followed all our guidance, but an independent review might show up issues that you didn’t consider.
* **Free cyber insurance** - Cyber Essentials certification includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation and have less than £20m annual turnover (terms apply).

## What accreditations are available?

**Cyber Essentials (CE)** – this looks at the fundamental controls which every company should be working to. Companies complete a questionnaire style form which is reviewed by a Cyber Essentials accreditor, like our [Trusted Partners](https://www.ecrcentre.co.uk/trusted-partners).

**Cyber Essentials Plus (CE+)** – this standard requires a penetration test in addition to the questionnaire of CE. If you don’t know what this is, a cyber security expert carries out physical tests against your network and computers. Successful accreditation of Cyber Essentials Plus provides a higher level of assurance that your organisation has a strong cyber resilience regime with correctly implemented controls in place to maintain a robust defence against cyber-attacks.

**ISO 27001** – this standard builds on and goes further than Cyber Essentials, looking at the whole of your Information Security Management System (ISMS) including those held on paper. It is a risk management system.

If you haven’t considered obtaining CE previously, why not have a look at the question set which is available to download for free from ISAME, who run the CE accreditation scheme. If you are ready to get the accreditation, then let us know and we can refer you to a Trusted Partner close by who would love to help.

And if you already have the standard, well done but remember that this is a point in time snapshot of your systems, just like your yearly car MOT. Once you drive it out of the garage your lights might break and it’s no longer roadworthy. Which means that you need to review your devices and systems on an ongoing basis and keep up to date with what’s going on in the world of cybercrime. Luckily that’s what our community is here for.

