Guide to Cyber Hygiene

Understand Your Risk

- Decide who on your Board (or senior manager in your company if you have no board) is responsible for managing the risk. Work out how much risk you face and how much risk you want to take. The IASME self-assessment questionnaire can help you do this. If you would like to be sent this questionnaire free of charge then please contact us.
- Identify your most valuable information in the company and mark documents containing this data clearly as "confidential" or similar.
- Create a policy describing what you want to do to manage the risk and include all the steps here. Distribute the policy to your staff. Review the policy regularly to ensure it meets your needs, particularly after expanding your business, acquiring a new partner or changing your supply chain.
- Allocate security responsibilities clearly to other staff and ensure staff understand the importance of working securely.

Teach Good Practice

- Write down what you want to protect in a policy or similar and make dissemination of this part of your induction process for new staff and compliance with the policy part of staff contracts.
- Remind staff regularly about good security practices, especially when the risk or the policy changes. Particularly make sure they know not to click on links in emails from unknown sources and report suspicious activity quickly to your risk manager.
- If you use social media for business purposes, you should ensure that all staff know that no sensitive material, intellectual property (IP) or similar material should be disclosed and that users behave responsibly while using social media for business or personal use, bearing in mind that they directly or indirectly represent the business

Protect your Network and Devices

- Find out if the router supplied by the Internet Service Provider (ISP) has a firewall built in and make sure it's operational. Change the access password if it's "admin", "password" or anything easily guessable. Limit who knows the password to those who really need to know.
- Install modern proprietary security software from mainstream suppliers like Symantec, Sophos, Kaspersky etc. on your PC/MAC and laptops etc. Follow the instructions to keep it automatically configured and updated. Preferably use a suite of software which includes anti-virus, anti-spam, identity protection and other protection because they are generally easier to manage.
- Use the 'on access' anti-malware facilities (it checks each time you open a file) and use the 'on demand' anti-malware facilities to sweep your devices at least once a day.

- Ensure your operating systems and applications are set to update automatically.
- Take note of any warning messages which are generated by the software and follow the guidance offered.
- Consult an expert if you think your network has been compromised. You might know this had happened if you noticed unusual activity - such as unusually high or low activity.

Manage IT Access

- Employ usernames and good passwords to control log-in. Good passwords contain upper and lower case characters, numbers and symbols and have 8 or more characters.
- Don't write passwords down or share them between users. Use different passwords for each application. Some security software providers offer password 'vaults' which allow complex passwords to be generated and then stored in an encrypted form, so you don't have to remember them.
- Limit admin privileges to those who need them.
- Ensure staff only have access to the folders they need to see. Keep sensitive data separate from the rest. There are innovative, simple and relatively cheap ways to keep sensitive data secure, e.g. hardware encrypted storage devices which connect by USB to your desktop or laptop device.

Keep Your IT Up-To-Date

- Document your IT assets so you know what you've got. IT assets will include hardware, software and even key IT staff.
- Install current software and operating system patches, firmware updates etc. immediately they are issued. You usually get this option when you install the software or you should find it in the configuration menu. Ensure all software is licenced.
- Check for technical weaknesses regularly (e.g. vulnerability or penetration testing). Regularly would mean when you update the risk assessment, perhaps annually or after major change of hardware or software.

Removable Media

If you transfer data using CD, DVD, USB, SD or any type of flash memory drive:

- Only permit business issued and controlled devices in your business systems
- Issue, retrieve and track the devices - know where they all are, who has them and, ideally, what software is on each.
- Ensure they are encrypted (some removable media devices already have encryption software on them) and scanned for malware on each use. Many commercial anti-malware packages (anti-virus) have the ability to scan removable media.

Mobile Working

Use of mobile devices for business purposes (privately or business owned) should require Board-level approval. Such devices must at a minimum have

- anti-malware software installed and updated daily (this can be set to happen automatically)
- pin, password or other authentication installed,
- be encrypted wherever possible and
- be capable of being remotely tracked and wiped.

All of the above can usually be done at little or no cost without technical expertise. Many of the mobile devices, particularly the newer models, can do this and you can set it up through the options or set-up screens.

- Staff should inform the Board-level risk owner (see above) immediately if the device is lost or stolen, and the device must be remotely wiped.

Monitoring

- Monitoring can detect potential hardware faults and unusual activity on your network or internet-connected devices. Modern laptops often come with the former installed and some anti-malware packages also have the latter.
- If your business has a large network you should use network management tools to detect unusual activity. This includes monitoring traffic flow, IP usage etc.
- Ensure that your staff report unusual activity to a central point and that you have sufficient plans and expertise on hand to react quickly.

Incident Management and Business Continuity

- Prepare for loss or compromise of your data by backing it up regularly (e.g. daily or at least weekly). Backups should be stored outside the office or in the cloud, but make sure that backups of sensitive data are encrypted.
- An attack should be flagged by the firewall or security package. Anything which interferes with the business is an incident.
- Decide what to do (and who does it) if you have an incident such as a malware attack, loss or corruption of data, laptop theft etc. and document it with the approval of the Board.
- Get in-house or outsourced expertise ready to deal with your incidents. Just knowing of a company with the relevant skills so you can call them quickly is important.
- Document any incident and decide what caused it, how much it cost to fix and whether there is anything you could do better in future.
- You should ensure that you know what to do (and document the actions to be taken) on the catastrophic failure of anything critical to your business such as information, applications, systems or network. Don’t wait for an incident to try out the plan.

Using the Cloud

- Remember that all data stored in the Cloud or processed using Cloud-based applications is available to the bad guys.
- Where you use data storage, applications or other services which are provided by another business (e.g. a ‘cloud provider’) you should choose one that has security which has been independently audited (e.g. certified to ISO 27001 or

IASME). You can find this out by looking for details of accreditation on their website or contact them and ask. Do make sure to ask the scope of the certification as some companies will accredit a small aspect of their business and then it may appear that the whole business is accredited.

- The use of the cloud should be treated like any other out-sourced provision and (ideally) be subject to service level agreements. You can contact them and ask for a Service Level Agreement.

- Do ensure that you know where and how your data is stored on the cloud and who is liable / responsible for that data. A particular issue is the country where the data is stored, which will have repercussions legally as anything stored outside of Europe requires different procedures. The cloud company may be based in the UK but have data stored anywhere and could even sub-contract it out to a third party. Even though the content of a website can be seen worldwide it is the location of the storage that is the legal requirement.

- An alternative approach might be to encrypt sensitive material using free or low-cost commercial software before it is sent to the cloud storage and share it (if required) by sending the password to the intended recipients' mobile device. Check that the device is currently in the recipient's possession before doing so and require the recipient to delete the message after use.