Defining and communicating your Board’s Information Risk Regime is central to your organisation’s overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

10 Steps to Cyber Security

1. **Secure configuration**
   - Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

2. **Network Security**
   - Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

3. **User education and awareness**
   - Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4. **Malware prevention**
   - Produce relevant policies and establish anti-malware defences across your organisation.

5. **Removable media controls**
   - Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

6. **Set up your Risk Management Regime**
   - Assess the risks to your organisation’s information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

7. **Managing user privileges**
   - Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

8. **Incident management**

9. **Monitoring**
   - Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

10. **Home and mobile working**
    - Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to [www.ncsc.gov.uk](http://www.ncsc.gov.uk)  @ncsc