Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: Survey, Delivery, Breach and Affect. The following security controls, applied at each stage of an attack, can reduce your organisation’s exposure to a successful cyber attack.

**Survey**
- **Patch Management**: Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.
- **User Education**: Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

**Delivery**
- **Malware Protection**: Malware protection can identify any malicious or unusual activity.
- **Secure Configuration**: Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

**Breach**
- **Device Controls**: Devices within the network should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.
- **User Training**: User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

**Affect**
- **Network Perimeter Defences**: Can block insecure or unnecessary services, or only allow permitted websites to be accessed.
- **Password Policy**: Can prevent users from selecting easily guessed passwords and lock accounts after a low number of failed attempts.

**Statistics**
- **81% of large companies reporting breach**
- **£600K - £1.15m average cost of security breach**


Who might be attacking you?
- Cyber Criminals interested in making money through fraud or on the sale of valuable information.
- Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.
- Hacktivists who wish to attack companies for political or ideological motives.
- Employees, or those who have legitimate access, either by accidental or deliberate misuse.