

# What you can do to combat 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

# **Delivery**

## **Breach**

# **Affect**



#### **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.



### **Network Perimeter Defences**

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.



#### **Malware Protection**

Can block malicious emails and prevent mailware being downloaded from websites.



## **Password Policy**

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.



## **Secure Configuration**

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.



## **Patch Management**

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.



#### Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.



#### **Malware Protection**

Malware protection within the internet gateway can detect malicious code in an important item.



### **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.



#### **User Access**

Well maintained user access controls can restrict the applications, privileges and data that users can access.



### **User Training**

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.



#### **Device Controls**

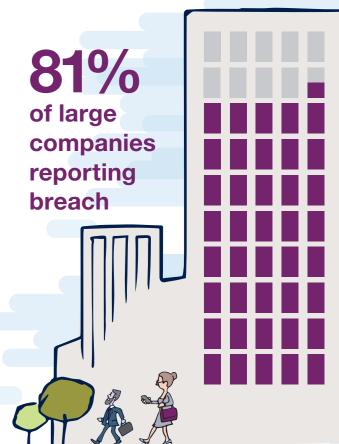
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.



## Controls For The Affect Stage **Controls For**

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.



## Who might be attacking you?



Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

from the sale of valuable information.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.



Average cost of security breach

