CPNI Personnel Security Maturity Model

EXCELLENT (Level 5) Low vulnerability

CURRENT BEHAVIOURS - The prevention of PerSec incidents is a core company value, and a board level member of staff has overall responsibility for PerSec. Security is part of "business as usual". The organisation recognises that the next threat is just around the corner and the PerSec risk assessment is reviewed at least once a year. Uses a range of indicators to monitor performance; but not just those which are performance driven. Organisation has confidence in its security processes and is constantly striving to find better and innovative ways of improving security control. All staff share belief of personal responsibility for security. The organisation is at low risk from operational, financial and reputational damage due to personnel security threats

DESIRED BEHAVIOURS - Develop consistency, implements a testing regime to help fight complacency. Regularly questions the effectiveness of security arrangements.

EFFECTIVE (Level 4) Medium/Low vulnerability

CURRENT BEHAVIOURS - The Executive board recognises that security is important from a moral and economic point of view, and can provide business advantage. Governance arrangements are as concerned with monitoring and influencing precursor indicators as with lagging indicators. Majority of staff accept need for personal responsibility towards security. The importance of all employees feeling valued and treated fairly is recognised. The organisation puts significant effort into proactive measures to prevent security incidents. Security performance actively monitored, and statistics collected and analysed. The organisation is at medium/low risk from operational, financial or reputational damage from personnel security threats.

DESIRED BEHAVIOURS - Engage all staff to develop cooperation and commitment to good security behaviours

COMPETENT (Level 3) Medium vulnerability

CURRENT BEHAVIOURS - There is an organisation wide consistent approach to security with defined processes in place. Organisation recognises the involvement of front line staff in security is critical. Managers recognise wide range of factors influence security & root causes can originate from management decisions. Significant numbers of front line staff willing to work with management to improve security. The organisation is medium risk from operational, financial and reputational damage from personnel security threats.

DESIRED BEHAVIOURS - Realise the importance of security from a social responsibility perspective and the importance of all staff accepting their personal responsibility for security.

DEVELOPING (Level 2) Medium/High vulnerability

CURRENT BEHAVIOURS - Personnel Security is seen as a business risk, given management time, and effort is put into reducing security incidents. Security still defined in terms of adherence to rules, procedures and technical controls; however there is an acknowledged approach using standardised templates. Security performance is measured in terms of lagging indicators (number of breaches, alarms). The organisation is at medium/high risk from operational, financial and reputational damage due to personnel security threats.

DESIRED BEHAVIOURS - Evolve from a purely reactive and rule-governed regime to a more proactive, anticipatory one. Develop precursor indicators, and front line staff to develop personal responsibility.

AWARE (Level 1) High vulnerability

CURRENT BEHAVIOURS - Personnel Security is defined in basic terms of technical or procedural solutions to meet UK employment legislation or regulation. No standardised threat mitigation processes, training or policy. No senior, board level, member of staff has been given responsibility for PerSec. The organisation is at high risk from operational, financial and reputational damage due to personnel security threats.

DESIRED BEHAVIOURS (TO MOVE TO NEXT LEVEL) - Develop management commitment to managing all aspects of protective security. Prioritise organisation's security risks and identify control measures for high risk threats.

INNOCENT (Level 0) High vulnerability

CURRENT BEHAVIOURS - Organisation is functioning at the most basic level. There are no formal personnel security policies, training or procedures. Senior Managers are unconcerned with the risks posed by people and have made no attempt to engage with CPNI. The organisation is at very high risk from operational, financial, and reputational damage due to personnel security threats.

DESIRED BEHAVIOURS (TO MOVE TO NEXT LEVEL) - Engage with CPNI