5 WAYS TO ACHIEVE A RISK-BASED SECURITY STRATEGY

Benefit from a strategy that naturally delivers compliance as a consequence of an improved security posture.

ASSET VALUATION

Determine what your key information assets are, where they are and who owns them. Think about business impacts such as lost revenue from systems going down or reputational damage caused by a website being hacked.

IDENTIFYING THREATS

Identify who may want to steal or damage your assets., why and how they may do it. Consider competitors, hostile nations, disgruntled employees /clients, activists, terrorists and non-hostile threats such an untrained employees Also consider natural disasters such as fires and floods.

IDENTIFYING VULNERABILITIES

Penetration testing and automated vulnerability scanning tools can help identify software and network vulnerabilities, but physical vulnerabilities need to be considered too. Are perimeters secure and controlled, are fire extinguishers regularly checked and backup generators tested?

RISK PROFILING

Risk profiling evaluates existing controls and safeguards and measures risk for each asset-threat-vulnerability and then assigns it a risk score. These scores are based on a combination of the threat level and the impact on the organisation should the risk occur.

RISK TREATMENT

Once each risk has been assessed, a decision is made to treat, transfer, tolerate or terminate it. Document each decision along with the reasons that led to it. Repeat the process for each threat scenario so resources can be applied to the risks that will likely be the most significant threat to the business

ComputerWeekly.com