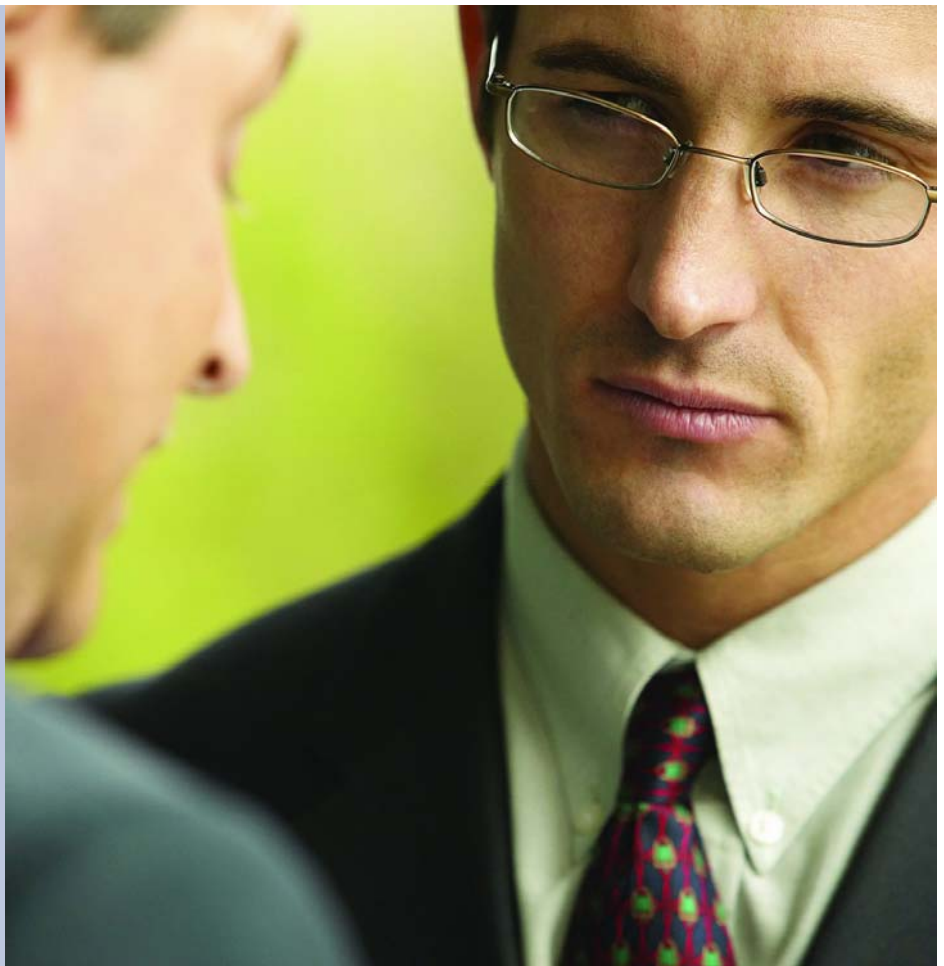


Product Application Profiles:

Using CRAMM to Justify Security Investment



CRAMM provides tools that can help with justifying investment in security

Where a particular security solution is under consideration, CRAMM can assist with helping to identify the risks that the security solution protects against, assessing the levels of risk and drawing conclusions on whether or not the solution can be justified.

This information is vital in determining how and where security budgets should be spent in order to ensure maximum return on investment.

CRAMM Express Worked Example:

A global company is implementing a new financial reporting system to be used from all locations worldwide. Group policy requires two-factor authentication for access to confidential information, but providing this solution to all users will be very expensive. Can the two-factor authentication solution be justified?

CRAMM Express was used to help identify the risks that two-factor authentication protects against - a range of masquerading and unauthorised use risks from several sources. The potential business impacts that could result from these risks were assessed in a small workshop with the business owner and

project manager for the new financial reporting system. It was established that whilst the financial reporting information was classified as confidential, the financial budgets for future years, also supported by the system, were much more sensitive and that serious financial damage could result if these were disclosed in an unplanned or unauthorised manner.

A second small workshop was held with members of the project team and information security team to assess the level of threat, level of vulnerability and the controls already planned to mitigate the risks.

Information gathered from the two workshops was entered into the CRAMM Express software tool which was used to calculate 'measures of risk'. These measures of risk were then compared against those for the 'two-factor authentication' solution held in the CRAMM countermeasure database. The conclusion from the CRAMM Express risk assessment was that two-factor authentication could not be justified for all users but that it was required for the relatively small number of headquarters

SIEMENS

Global network of innovation

