M&M 950

Platinum SQUARED

Risk Assessment - Determining the Risks

What is Risk Assessment?

Every day we all conduct numerous risk assessments probably without even realising that we are doing so, for example, where should I cross the road?, should I buy a cheaper item which might be less reliable? All of these involve making assessments about the possible threats, the potential impacts and the costs involved in taking the possible precautions. We do these risk assessments instinctively and almost instantly. However, when we are talking about the security of information, there are many people who may have an interest in protecting the data, each of whom may have different views on the risks and what would represent the 'appropriate' controls. Ultimately the best way to reach agreement is if the organisation documents and agrees its views on the risks to the information and the protection it should put in place against those risks, i.e. conducting a risk assessment.

Why Do it?

As documented in ISO 27001, performing a sound risk assessment is critical to establishing an effective Information Security Management System (ISMS). The risk assessment should provide the framework for establishing policy guidelines and identifying the necessary controls and procedures that the organisation needs to implement.
The risk assessment is necessary to ensure:

- The assessment of threats, vulnerabilities and potential impacts has been conducted in a comprehensive and objective manner.
- The conclusions reached about the requirements for security can be agreed by all parties involved.
- There is a common basis on which to discuss the need or otherwise for particular countermeasures.
- The results have been documented in such a manner that they can be shared with people, such as external auditors, who have not been involved in the original assessment.

Why does the Risk assessment have to be a formal method?

Reliably assessing information security risks can be more difficult than assessing other types of risks because the value of the data can be difficult to assess, the range of threats varies from the simple, such as user error, to the highly technical, such as cross site scripting attacks, and the range of controls that need to be considered is constantly changing. The method has to be formal because:

- It needs to be 'repeatable', so that if two people were to conduct a risk assessment on the same system they would identify the same problems.
- The results should be based on known and accepted standards.
- The results may have to be explained to people from outside of the organisation, as well as people inside the organisation.

How Risk Assessments are conducted?

As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being considered, risk assessments generally include the following elements:

- Identifying threats that could harm and thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will occur based on historical information and the judgement of knowledgeable individuals.

How Risk Assessments are conducted? continued.

- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat occur, in order to determine which operations and assets are the most important.
- Estimating the potential losses or damage that could result if a threat were to occur.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organisational policies and procedures as well as technical or physical controls.
- Documenting the results and developing an action plan or a 'security case'.

There are various models and methods for assessing risk and identifying the appropriate controls. Platinum Squared has significant experience in many of these methods, in particular:

- HMG Information Assurance Standard No. 1.
- CRAMM Expert and Express.

How can Platinum Squared help?

Platinum Squared's has extensive experience, gained from conducting hundreds of risk assessments, in both the Private and Public sectors and can help conduct risk assessments quickly and effectively.

Platinum Squared's team includes the consultant who led the work on developing CRAMM, which is a UK Government's recognised approach to risk assessment, and therefore has knowledge not only of how to complete a risk assessment, but also the theories behind the risk assessment methods.

Platinum Squared has put together bespoke training courses on how to conduct risk assessments in accordance with HMG Information Assurance Standard No. 1 and foundation courses in understanding the risk assessment process.

Summary

Evidence from organisations that have used formal risk assessment programmes indicates that such work is important in supporting their business activities and provides several benefits.

Firstly, and perhaps most importantly, risk assessment programs help ensure that the greatest risks to business operations are identified and addressed on a continuing basis.

Secondly, risk assessments help personnel throughout the organisation better understand the risks to their business operations; giving them the motivation to avoid risky practices, to be alert for suspicious events and to support security improvements.

Platinum SQUARED

Platinum Squared Limited - Bedford iLab • Stannard Way • Bedfordshire • MK44 3RZ
tel: +44 (0)1234 834596 • email: info@p2.co.uk • web: www.p2.co.uk • twitter: @platinumsquared
Registered Company No: 05586975 • Registered VAT No: 942 3403 45