Good security plan and implementation memo research proposal example

Law, Security

Return On Investment (ROI)This is the expected return under a normal network state. ROI (Gain by investing – Cost of investing)/ Cost of the InvestmentROI = ($40, 000 - $25, 700) / $25, 700 * 100% = 55. 64%Retina scanners This is a security technology that uses the iris scan technique, to scans for retina properties of desired individuals. It does this by scanning on unique eye properties such as the eye properties, and blood vessels, which are is registered on that particular device. It scans using light and is commonly used for identification and authentication purposes (Newman, 2010). Return on InvestmentAccess control device CostIris recognition access control system $15, 000Deployment cost $1000This is the expected return under normal access to premisesROI (Gain by investing – Cost of investing)/ Cost of the InvestmentROI = ($20, 000 - $16, 000) / $16, 000 * 100% = 25%Smartcards These are smart cards, of relative size to an ATM or credit card that is used to store security data as pertains access to a given place. It contains some metallic component that contains data of an individual, in which the individual taps on an access device, reads the information and grants or denies the person access to the premises (Honey, 2000).

Return On InvestmentAccess control device CostSmart card access control system $10, 000Deployment cost $2000This is the expected return under normal access to premisesROI (Gain by investing – Cost of investing)/ Cost of the InvestmentROI = ($20, 000 - $12, 000) / $12, 000 = $66. 67%

Significant sizes in terms of the role played by the security devices

Risk mitigation: This is an approach that is used to manage the likelihood and impact of future related risks (Menoni & Margottini, 2011). This is achieved by carrying out a study on the current situation, and including the missing items in order to contain any future potential hazard. In order to mitigate the risks, the security department will update the Chief Information Officer on the progress of the deployed devices. This will facilitate internal reviews aimed at finding vulnerabilities, upon assessment in order to prevent potential network breaches. Barriers to success These are factors that may hinder the success of the planned inclusion and deployment of these security technologies. These factors will hinder the success in the adoption of these gadgets, especially when it is internal. When an organization is not fully involved and committed to the technologies. There are inadequate funds set aside, annually to review all security measures, technologies in order to facilitate upgrades, in case of inefficiency.

References

Honey, G. (2000). Electronic access control. Oxford: Newnes.

Komar, B., Beekelaar, R., & Wettern, J. (2003). Firewalls for dummies. New York: Wiley Pub.

Menoni, S., & Margottini, C. (2011). Inside risk: A strategy for sustainable risk mitigation. Milan: Springer.

Newman, R. (2010). Security and access control using biometric technologies. Boston, Mass: Course Technology.

Friedlob, G. T., & Plewa, F. J. (1996). Understanding return on investment.

New York: Wiley.