Information security management system (isms) in a company

Business, Company

TechnologyOutlook Express is used for mailcommunication. The company must use a range of multimedia software to produce printed goods. The company has two computers one of which is High Spec used for accounting and ordering and the other for the printers. Information security management system is a set of policies connected with information security management and information security risks. The expressions came from ISO 27001. " The principle behind ISMS is that an organisation should design, implement and maintain a clear set of policies, processes and systems to manage risks to its information assets, therefore ensuring acceptable levels of information security risk."

ISMS should be competent in the future and should adapt to changes whether they are internal or external and therefore should integrate the Plan-Do-Check-Act cycle method which will keep it up to date. From the above the company will determine whether it is cost beneficial to place for example a lock on the stationary room, if the lock cost more than the stationary then it can indeed be seen as useless reason being that the stationary can be replaced if stolen this would be a cheaper alternative to buying a lock. But a lock could act as a deterrent to stop the theft in the first place.

Web hosting as the site is not hosted by the company is it secure and safe, is it vulnerable to attack from the web hosting side. Secure passwords should be used which use a combination keyboard keys, it is also vital to see what security measures the hosting company has in place. If a hacker gets control of the company's website then secure card details are at risk. Online sales

are being processed through the website are the credit/debit card details and customer details safe and are they being encrypted e. g. SSL, where are the details being saved and who has access to them. Is the website secure e. g. VeriSign secure SSL or MacAfee hacker tested?

Are there any validations on computerized processes that are completed by employees to reduce human error, e. g. a form would only allow alphabetical letters and not allow numbers in certain text boxes such as 'Name' to avoid errors, or have drop down combo boxes for dates. Data protection is also vital as data should be protected either by access control, encryption and passwords. Only allowing the accounts department access to employee payrolls would increase data protection as the risk of data theft, loss and corruption occurring is reduced. As well as that the company needing to check whether the customer data is secure and employee data is secures as well as it being backed up regularly.

The company should be ready for any threats from nature; these can include floods, hurricanes/tornadoes, and earthquakes. Each of which can have a devastating effect on the company from taking out the power to destroying the premises where they are based, threats such as these are rare and should be based upon the history of the area in which the premises are located, if near a river then floods could be likely and computers and printers should be placed above the ground floor. Power generators should be used to stop powerfailurein case of power cuts, but most importantly premises and content should be insured in case of major disasters which could bring down the company.

Software Attack Virus protection is vital to fight the threat of software attacks regular updates should be checked for and important patches should be installed for the OS. An IDS would detect if any attack was being made and alert the appropriate person to the attack. A 'Honey pot' (a decoy system fabricated with useless data) should be deployed to deter hackers to it allowing the IT Security Manager to see where the hack is originating from and to block it.

Premises The premises should have locks on doors, CCTVand alarmed so that the data on the computers inside the premises is secure and reasonable steps have been taken to secure it Conclusion: Overall to comply with ISO 27001 the company needs to start looking at risks starting within the company itself, the employees are the most likely risk, steps should be taken to implement access control to the current system. The external system should be secured by means IDPS, if that is not possible a firewall should be put in place to secure the system and configured for the company's requirements. The website should be secured if not already even if this means moving to a different host, loosing customer data to hackers could mean a drop in sales as customers will not believe their data is safe within the company, the company being sued under the Data Protection Act 1998.

References:

http://security. practitioner. com/introduction/infosec_4_4. htm