Gdi consulting firm security policies research paper examples

Business, Company

1. Introduction:

Legally named as ADI Consulting, GDI Consulting & Training Company functioning as a DBA (Doing Business As) of Gerald E. Dunn, Inc. provides corporate solution to complicated business and administrative problems in manufacturing and distribution industries. It has been in the business for last 30 years having implemented solutions in 18 different countries for over 200 clients. GDI Consulting initiated its business way back in 1980, chiefly as a consulting firm assisting manufacturing and distributions industries with solutions relevant to the problems of the implementation of information systems, supply chain and business makeover issues.

Typically, the company handles lot of client data during its project engagements. In many cases such data are sensitive and important to the client. GDI and its employees often need to handle them carefully and distribute with caution so that the privacy of those data can be maintained. This often is a cost intensive affair to hold sensitive data securely. GDI needs to have encrypted storage mediums to store the data, multiple layers of firewalls to block hackers and training sessions to employees to educate how to handle sensitive information. If GDI does not follow such strict policies for data protection, the consequences may be even more cost intensive in terms of giving compensation to the client for the damage incurred by mishandling and theft of sensitive information.

If GDI can establish itself as a reliable organization that handles client information with great care then more and more clients will be drawn to making business deals with GDI in full knowledge that the consulting partnership with GDI will be dealt with utmost care and responsibility.

2. Elements for Effective Security Policy:

Security Policy in business refers to the security measures undertaken by a company in protection of its physical as well as IT assets. The current security challenges encountered by GDI make it imperative for the company to install firm security policies. The key elements for effective security policies include Facility and Physical Security Policy, Information Systems Security Policy, Personnel Security Policy, Ethical and Moral Policy, Acceptable Use Policy, Safety and Health policy, Business Continuity Policy and Email and Communication Policy.

- Facility and Physical Security Policy

Physical Security involves security measures designed to deter physical entry of unauthorized individuals to protected facilities and controlled peripheries of an organization. An array of physical access controls including alarms, access badges, barrier, CCTV, CPTED, intrusion detection, lighting, lock and security guard patrols should be installed by GDI to tighten its physical security. Access of unauthorized personnel could be prevented by issuing of access badges to the employees and visitor badges to non-employees who will sign their names and register the purpose of their visit at the entry point and will return the badges once their visit is over. Some common forms of CPTED to deter access of potential threats inside the campus or building of an office involve security lighting, fences, window stickers, vehicle height restriction and trenches. Alarm systems notify immediately of an intrusion attempt via triggering the sensors such as motion sensors and contact sensors. CCTV that monitors the activities of people inside and outside the building also helps in identifying the intruders.

Security guards are responsible for taking patrols, identifying and interrogating suspicious people and quickly responding to alarms in case of emergency.

- Information Systems Security Policy:

In an era of Information technology when IT assets are susceptible to malicious cybercrimes including theft, misuse and destruction of sensitive data and disruption of internal system, means of computer security should be strengthened by GDI Consulting Firm. Technical control monitoring and restricting access to information and internal system should be instituted via passwords, data encryption, firewall, VPN and router. Internet access policy should be supported by a layer of authentication and authorization implemented via PIN, password, security questions, swiping of driver's license, biometrics including finger prints, eye scan and voice print before allowing access. State of the art tools and software should be installed to determine network vulnerabilities of GDI and threat assessment as precaution against any harmful breach of confidential database. There is a host of DLP software available in the market that can be implemented in order to prevent breaching or illegal transmission of data. Further, a good back up strategy through a combination of full backups and incremental backups should be undertaken to prevent the loss of important information and data. Guest network should be secured with wireless routers. Account lockout feature should be implanted in the event of a password being entered over a specified number of times.

- Personnel security policy

- Ethical and moral policy

There should be some set principles of ethical and moral standards for the employees of GDI Consulting Firm to adhere to. Employees must be educated during the orientation about the importance of keeping privacy, honesty and integrity in the execution of their roles and responsibilities. Managers entrusted with the responsibility of formulating these organizational principles should be obligated to make sure of the policies being implemented.

- Acceptable use policy

Acceptable Use Policy (AUP) refers to a policy implemented by many institutes as well business organizations to make the user sign or agree to some guidelines before allowing access to a network or database. GDI Consulting Firm in order to safeguard itself from potential threats must put AUP into work by making the employees sign the contract of non-disclosure agreement (NDA) and company compliance agreement with consequences written in clear terms in case of a breach of the policy. Further, the intellectual property of proprietary methodologies or intellectual knowledge capital that are owned by GDI but shared with third parties during implementation of a project should be secured with proper licensing and acceptable use policy.

- Business continuity policy

Business Continuity Policy (BCP) preserves the continuity of critical business functionalities without stoppage regardless of untoward incidents or circumstances. A good BCP insures the stability of a company in the face of hazards and adverse situations. Emergency situation come uninvited and therefore, GDI must ready itself to overcome any hazardous situation by

putting Emergency Response Plan, Incident management plans, Crisis management plan and Disaster recovery plan into action. Emergency Response Plan, a subset of BCP, refers to the actions for safety taken during an emergency such as evacuation, shelter, shelter-in-practice and lockdown. Incident management plan describes the insightful action taken by a company to prevent the recurrence of a hazardous incident by identifying and analyzing the situation in which the hazard took place and taking correct measures to prevent the recurrence. Crisis Management is a process that classifies crises based on type into different groups and employs different strategies to deal with each specific crisis. A disaster recovery plan records the procedures to follow before, during and after a disaster in form of writing. This plan is broadly associated with the recovery of IT assets, data and facilities.

- . Email and communication policy

GDI also should focus on strengthening the email and communication policy by installing effective antivirus software that keeps harmful virus, bugs and tracking cookies from infecting the systems. In order to prevent fake emails, spoof and spam messages from clogging the systems, encryption of emails and digitally-signed emails should be made mandatory to protect confidentiality. Furthermore, GDI should train the employees to be careful of handling emails and encourage building of an environment where a two-way communication is exchanged.

Conclusion:

GDI Consulting Firm that has made its name in the business world by successfully providing solution to managerial and business related problems

in the manufacturing and distribution industries for over 30 years has security concerns related to dealing with confidential data during business engagements. In the era of information technology when business ventures are dependent on the use of internet, stealing of sensitive information, hacking, gaining access to private information are not uncommon. Hence, in order to solidify its business security, GDI plans to institute an array of security measures to protect itself from any uncalled-for security infringement. The most effective measures to reinforce security involve physical security, information systems security, personnel security, ethical and moral policy, acceptable use policy, business continuity policy and email and communication policy. By taking these security measures GDI can safeguard itself from any potential danger coming in the form of natural or man-made disasters. However, though no security measure can be 100% full proof, these security measures by creating a bulwark will make malicious attempt at security breach difficult to pull through.

References:

- History & Organization of GDI Consulting & Training Company, By Alan G. Dunn, President http://www. gdiconsult. com/BackgroundHistoryOrganization/tabid/151/Default. aspx (11th April, 2013)

- The Six Pillars of Personnel Security Policy, Information Shield http://www. informationshield. com/security-policy/2012/12/the-six-pillars-of-personnel-security-policy/ (11th April, 2013)

- Brush up on personnel security, http://searchsecurity. techtarget.

com/tip/Brush-up-on-personnel-security (11th April, 2013)

- Security policy, http://searchsecurity. techtarget. com/definition/security-policy (11th April, 2013)

- http://delawareasis. org/uploads/Facilities_Security. pdf (11th April, 2013)

- Cyber Security, BG Tech, http://www. braxtongrant. com/vulnerability-and-threat-assessments. html (11th April, 2013)

- Backup Tips - Prevent data loss with a good backup strategy, iOmega, http://iomega. com/data-recovery/prevention-backup-strategies. html (11th April, 2013)