Bogart a case in point

Bogart – A Case in Point

Case Background

Senior management of Bogart Engineers and Constructors, Inc. is faced with the dilemma of defining clear IT management practices that would prevent breach of security, tampering of files, and stolen files instigated by two computer programmers, Roy Johnson and Jerry Williams. Specifically, the case required ten recommendations with explanations on strengthening IT management practices to ultimately prevent future security breach.

Recommended Courses of Action

1. Review and evaluate corporate policies and procedures on the use of both computer hardware and software and determine the need to revise and amend areas that need focus, especially involving the use of critical information programs and systems. Policies in recruiting new IT personnel must likewise be strengthened in terms of background checking for past working experiences, qualifications and credentials.

2. Design and implement a code of discipline complete with sanctions for violations of policies. Appropriate sanctions for employees found to violate such policies should range from reprimand, warning, suspension, expulsion to outright firing, as required.

3. The current status of computer hardware and software systems at Bogart need to be protected in terms of confidentiality clauses and current employees directly using these systems must sign an official agreement that they abide by the policy of secrecy and confidentiality, otherwise, the sanctions indicated in the Code of Discipline, should be strictly enforced.

4. Categorize the computer hardware and software systems in terms of

crucial importance to the organization. Those identified highly classified should only be used by authorized and trusted personnel whose trust has been gained by senior management through lengths of service within the company.

5. Clearly identify responsibilities and restrictions of personnel who should only be authorized to use systems which were classified according to levels of confidentiality.

Any unauthorized personnel should be prevented to access critical programs by assigning codes and personal access numbers.

6. The practice of allowing personnel to bring their workload at home and have the computers sourced from the office be linked accordingly should be immediately stopped.

If there are critical workloads that need to be finished at defined time frames, everything must be done within the premises of Bogart to prevent loopholes and to prevent compromising privacy and confidentiality.

7. Enforce strict monitoring and control of all computer resources through regular check-ups or audits to determine if there is any security breach at any points in time, or in any critical programs. Bogart could also incorporate it their policy the need to rotate authorized employees handling of critical programs to serve as a check and counter-check mechanism.

8. External audits must be scheduled aside from the in-house monitoring and control to ensure that programs are not compromised, tampered, or breached. Outside IT personnel who are constantly updated on the latest developments on security breaches are more abreast of details to identify any risks or threats involved.

9. Schedule regular orientation and training to new and old personnel on the

policies, practices and protocols for using computer hardware and software systems and programs at Bogart to enforce awareness and to instill discipline. Management must be serious in enforcing sanctions in cases personnel were found to violate policies. However, a reward system must likewise be given to employees who consistently adhere to standards and opt to improve the present system by identifying flaws and suggesting improvements.

10. Management must always be vigilant in ensuring that their IT management system is not compromised through direct and active involvement, monitoring, regular updates in information and equipment, personnel checking, and identification of signs that signal dangers in security breach.