Data case study

Business, Company

Programmer Ethics and Professionalism in Strategic Systems Development: A Case Study

A team of four programmers was given the task of developing new software to be sold Bogart Engineers and Constructors, Inc. Two of the programmers, Roy Johnson and Jerry Williams, took advantage of their position in the company as developers of Engineers and Constructors, Inc. proprietary software. The two programmers broke the seventh and tenth commandments of the 10 Commandments of Computer Ethics – ‘ 7 Thou shalt not use other people’s computer resources without authorization or proper compensation’ and ‘ 10 Thou shalt always use a computer in ways the insure consideration and respect for your fellow humans.’ The men were hired to develop software for the company and sold as the Bogart System. Instead they behaved unethically and unprofessionally. This paper addresses the question: What could have Bogart Engineers and Constructors, Inc. done to protect itself from the malicious actions of these two employees?

Here is a short and succinct list of the crimes that Johnson and Williams committed while employed with Bogart.

- The programmers continued accepting pay for their work from Bogart Engineers and Constructors, Inc. although the two men were developing the software to meet their own ambitious goals.

- The programmers violated the confidentiality agreement which they had signed when they accepted employment at Bogart Engineers and Constructors, Inc. Johnson and Williams had agreed to respect the proprietary claims described in the agreement. They had inserted a microdot into the programming which proclaimed ‘ Roy Johnson and Jerry Williams,

Copyright, 2003.’

- One of the programmers violated Texas Criminal Law by coding self-destruct instructions so that some modules of the software would crash. The commands that were encoded into the software would occur at dates and times scheduled in the future. Other damage was encoded into the B. I. D. project.

- Williams stole the software, documentation and data for the B. I. D. project using it as a negotiating leverage so he and Johns would receive their final paychecks. The B. I. D information was returned within 48 hours.

Bogart Engineers and Constructors, Inc. filed for legal action and in 2004 a settlement was agreed upon.

Human Resource Management (HRM) and Information Security Management (HRM) systems at Bogart Engineers and Constructors, Inc. were not prepared to handle the B. I. D. project from before the time of hiring programmers to develop the software; several glaring problems enhanced the problems the crime highlighted.

Access and Identity Management is only one component of internal computer security policy but by using a management system that stressed access and identity barriers to inapporpriat3e data would have saved Bogart Engineers and Constructors, Inc. both time and money. Administrative permissions and password updates to make sure that employees have the appropriate access to the information and data should have been a routine part of the operations. When employees have the appropriate access to computer files that means they do not have access to files that they should not be able to open.

Security Regulation policy was obviously lax at Bogart Engineers and Constructors, Inc. because a new security agreement was drawn up after the copyright infringement issue was brought to light. Johnson and Williams refused to sign the new agreement giving Bogart management a barrier to implementing any new security regulations with people already employed in the company. Bogart should have had their legal advisors review the security agreement and the security regulations the company was using before any new hiring took place.

Security Training and Awareness should have been a routine part of the ISM and HRM activities. This would have made the importance of computer security to the organization’s leadership and management transparent. Computer security improvements and developments increase quickly so the need for up-to-date training for employees is essential. The company could include books, reports and other information in the company library to help employees stay up-to-date. The company should also have workshops available on the site or access to seminars and workshops offsite should be made for employees.

Information Security Management (ISM) in the past concentrated on technological answers to security questions but the human factor causes the most security failures. That does not mean that Bogart should ignore administrative permissions and password updates to make sure that employees have the appropriate access to the information and data. Williams and Johnson should have had only the data they need to do their portion of the work on the team instead of access to all of the projects work. Role of Human Resource Management (HRM) in the organization needed to

be modernized so that the staffing practices of choices from applicants were accomplished with ISM input and an acknowledgement of the importance of ethics when making hiring decisions. For example when references were checked for applicants HRM needed to ask about the behaviors of the potential employee influence their ethical practices and decision-making. Integration of ISM and HRM is a strategy that could have been initiated at Bogart Engineers and Constructors, Inc. before the four programmers were hired to develop the new software. The reason the argument for integrating ISM and HRM is so strong is exactly because the large number of security failures caused by employees. The staffing and training needs in the information technology department are better understood by ISM and could enhance the HRM search for potential employees. For example someone from the IT department may understand the job history of applicants more easily than someone in the HR department.

Effective interaction between team members is clearly a place the company needed improvement before starting the project. The problem became clear when one of the four team members found the microdot with Johnson’s and William’s copyright embedded in the Bogart company logo. One of the newer management concepts that could help is called Transactive Memory Systems (TMS). Team members are the managers of information when using the TMS strategy. The team needs to understand who has the most expertise for what portion of the project (coordination), trust between team members is essential (credibility), and identifying the domain specialties of each member (specialization). TMS been shown to help project teams manage the general and special knowledge of team members because it “ match(es) people with

appropriate skills (and) maintains effective interactions among members, a combination which ultimately improves team performance" (Wipawayangkool 6). Wipawayangkool (2013) reported that earlier research has shown that geographic distance can have a negative impact at first but the need for the team members to share their expertise can overcome that problem.

Prevention of internal computer security problems should have been addressed. Yoon and Kim suggest using a model they created which includes the following features " theory of reasoned action (TRA), moral obligation, protection motivation theory (PMT), and organizational context factors" (401). PMT explains employee behavior as based on fear such as " perceived threat severity, response efficacy and employee's behavioral intentions of computer security" (Yoon and Kim 402); when integrated with the other three factors can enhance employee's behavior on the issue of computer security. The most important finding of Yoon and Kim's (2013) for Bogart was that the company's security policy affects employees. The Bogart company should have been communicating their computer security policy with awareness programs and training. Three major components for contemporary computer security that can be managed to avoid human factor computer security problems are " access and identity management, security and regulation compliance, and security training and awareness" (Wipawayangkool 1).

The Knowledge and Copyright Agreement that Bogart Engineers and Constructors, Inc. had the four new team members signed when they were hired was not adequate to impress upon Johnson and Williams the priority

place by the company on proprietary products. Perhaps that is because it was not a priority but certainly should be by now. The company had always been a service company but the venture into the software development sector was not well researched by the leadership and/or management before the programmers were hired to start the development project. Volpe and Schopfel (2013) have done research that warns of the complexities of the issues of knowledge and copyright issues in the scientific domain which also applies to technology.

Employee incentives for respecting proprietary property of the company and for responsible computer security activities were not adequate. Li and Xu (2013) have noted that a new philosophy for worker incentives can be developed based on features of human capital. The researchers have pointed out that the new philosophy incorporates the idea that employee's participation in the company in new ways. Li and Xu point out that " human-oriented management about employee's participation in management, stock option incentive mechanism(s), and career development" (1) have been developed to motivate and develop the skills and talents of knowledge workers. Demortier and Delobbe (2011) have pointed out that Knowledge Intensive Firms (KIFs) require different attitudes than other sectors; by adding software to their production goals, Bogart was entering the realm of KIFs so they should have learned more about the pitfalls that could occur.

The priorities of Bogart Engineers and Constructors, Inc. were not appropriate to reaching their goal of having a competitive advantage by offering their customers software developed in-house. The priority for the company appeared to be gaining an advantage over their competitors.

Bogart used the wrong strategies though to ensure success in reaching their goal by moving into the software development field. The company had not done their research on how to best address issues of computer security and proprietary issues. The company had not developed an organizational attitude and coherent policy on team work and along with that, the access to data for each of the team members. The company could have taken early action to discourage the behavior by redesigning HRM and ISM interactions, and change their communication of the firm's goals to the employees. They also should have had their Information and Communication Operations Manager strengthen computer security. IT security should not be focused on technology but on issues where employees interact with the technology (such as access to information and identity management), where the knowledge of employees can be enhanced by understanding security and regulation compliance policy in the company, and by offering employees consistent up-to-date opportunities for security training in order to keep the awareness of the priority of IT security within the company high.

Works Cited

Demortier, Anne-Lise and Nathalie Delobbe. " Human Capital and strategic human resource management in knowledge-intensive firms: an exploratory study", EURAM2011 – 11th Conference of the European Academy of Management, 1st – 4th June 2011, in Tallinn – Estonia www. uclouvain. be/cps/ucl/doc/crecis//2011-09_Demortier. pd

Li, Nai-wen and Meng-hong Xu. " The Research of the Knowledge Worker Incentive Strategy Based on Human Capital Characteristics", The 19th International Conference on Industrial Engineering and Engineering

Management Ed. Ershi Qi, Jiang. Shen and Runliang NY: Springer-Verlag Berlin Heidelberg (2013), pp 643-650 Web. 1 Nov. 2013.

Volpe, Tony and Joachim Schopfel, " Dissemination of knowledge and copyright: an historical case study", Journal of Information, Communication and Ethics in Society, 11. 3 (2013) pp. 144 – 155 Web. 1 Nov. 2-013. http://www. emeraldinsight. com

Wipawayangkool, Kamphol. “ Alleviating Knowledge Overload in IT-HR Collaboration in Information Security Management via Transactive Memory Systems.” Journal of Knowledge Management Practice, 14. 2 (2013): 16 pp. Web. 1 Nov. 2013.
http://www. tlainc. com/articl342. htm

Yoon, Cheolho and Hyungon Kim, " Understanding computer security behavioural intention in the workplace: An empirical study of Korean firms", Information Technology & People, 26. 4, (2013) pp. 401 – 419 Web. 1 Nov. 2013. http://www. emeraldinsight. com