PROGRAMMER ETHICS AND PROFESSIONALISM IN STRATEGIC SYSTEMS DEVELOPMENT: A CASE STUDY

By
Charles K. Davis, Ph.D.
University of St. Thomas
Houston, Texas
July, 2000

ABSTRACT
This article explores the vulnerability of business organizations to unethical, unprofessional, and even vengeful acts by employees who seek to damage a critical class of information systems: corporate strategic information systems. The case of Bogart Engineers and Constructors Inc. (disguised name) is presented. In this case, two programmer employees tried to claim ownership of a Bogart strategic information system and also sought to destroy the functional integrity of Bogart’s copy of the system. Computing systems that provide a business enterprise with competitive advantage demand senior management attention. Rigorously enforced standards in the selection and training of staff and in the management and monitoring of work performed on strategic systems is essential. This article provides recommendations for reducing business exposures associated with employee malfeasance relating to information systems technology.


PROGRAMMER ETHICS AND PROFESSIONALISM IN STRATEGIC SYSTEMS DEVELOPMENT: A CASE STUDY

In a “Sloan Management Review Forum” on ethics in business, Saul Gellerman (1989) asked, “How can organizations protect themselves from employees who behave unethically?” In the realm of information technology, this question might be rephrased, “How can organizations protect themselves from their own computer programmers who engage in unethical, unprofessional, even vengeful, misconduct?” This question takes on added significance when it refers to those employees who have access to a corporation’s strategic information systems.

This article deals with strategic information systems, the question of programmer ethics, and the potential
for serious consequences if strategically valuable information systems are compromised. The “real world” nature of this vulnerability is illustrated with the case of Bogart Engineers and Constructors, Inc. Bogart (a disguised name) became aware that two members of its programming staff were trying to appropriate a copy of one of Bogart’s strategic software systems. Also, at least one of the programmers involved had attempted to destroy Bogart’s own copies of the system. This case study presents how Bogart fought back. Implications for management are drawn from the Bogart experience. The article concludes with managerial guidelines for protecting strategic information systems from the kinds of risks illustrated by the case.

INFORMATION SYSTEMS FOR COMPETITIVE ADVANTAGE
Lederer and Mendelow (1988) define strategic information systems as those that help corporations accomplish “fundamental competitive objectives.” Such systems are crucial in sustaining the success of business enterprises. Growing corporate attention to, and dependence upon, strategic information systems dictates that executive management become more involved in the information systems area. Especially now, as corporations restructure for global competition and increasingly take advantage of information technology as a competitive weapon, successfully implementing strategic information systems is missioncritical for many businesses.

The Competitive Imperative. The loss, theft, or destruction of a strategic information system either during development or after it is operational has serious consequences for the competitive posture of a company. The amount of time, expense, and effort needed to develop a major information system is, of course, substantial. A company that must begin the systems development process anew faces costly and often demoralizing delays in implementation. With strategic information systems, such delays also can mean a weakened competitive position for the entire business enterprise. A delay may even eliminate any competitive advantage whatsoever when the completed system is finally operational. Delays give business rivals the time needed to counter the competitive impact of a particular system, perhaps erasing its strategic value altogether. Furthermore, with strategic information systems, it is extremely difficult to abandon a troubled project. Regardless of the amount of money that is lost initially, the basic competitive situation that mandated the original need for the system does not change just because the system has been compromised somehow.
The corporation is almost always compelled by business imperatives to proceed with development regardless of difficulties encountered along the way. The Role of the Executive. It has become axiomatic that leading corporations look for opportunities to construct business strategies around advanced information systems. They strive to use information technology strategically for competitive advantage in the marketplace. (Armstrong & Hagel, 1997; Callahan & Pasternack, 1999; Cash and Konsynski, 1985; Drucker, 1997; Evans & Wurster, 2000; Ives and Learmonth, 1984; Keen, 1986; King and Kraemer, 1989; McFarlan, 1984; McGee & Prusak, 1993; Mendelson & Ziegler, 1999; Porter and Millar, 1985; Rockart and Scott Morton, 1984; Wiseman, 1988a).

In fact, few today would argue with Henderson’s prediction (1990) that the effective use of information technology in competitive strategy has become the critical dimension for modern corporate success. While firms forge ahead with the development of strategic systems applications, executives are recognizing a significant new business risk. Employees who work with strategically valuable systems may, for whatever reasons, decide to harm the corporation by compromising key systems (DeMichiell, 1988; Drucker, 1999; Gellerman, 1989; Mason, 1986; Murphy, 1989; Rash & Yost, 1997). As business organizations strive for competitive advantage by incorporating strategic information systems into their portfolios of computer applications, the threat associated with the theft or destruction of key systems by employees who behave unethically should be a real concern for senior corporate management. Furthermore, the risk will only increase as strategic use of information technology proliferates into every aspect of modern corporate life and becomes increasingly more complex.

It is, therefore, clear that executives must play a part in managing this technology because of its strategic implications. Benjamin, Rockart, Scott Morton, and Wyman (1984) suggest that the role of senior management must be modified to include leading in the use of information technologies to facilitate, or even enable, corporate strategy. Information systems have become central to executive management’s ability to know where it currently is in the marketplace, where it wants to be in the future, and how best to get there. The strategic use of information systems poses a particularly thorny planning and control question for senior management. Organizations are highly vulnerable, as never before, to unauthorized, improper actions of one class of their own employees, the computer programmers. Programmers, who understand
how a system works internally and are technically capable of modifying the system, are the ones who can most effectively sabotage software and use pirated software in rival organizations. Furthermore, the level of exposure to programmer malfeasance continues to grow as strategic information systems applications proliferate. Executives must refocus their thinking accordingly and take action to assure the safeguarding of these uniquely critical resources. Failure to do so means corporate competitive viability itself is at risk.

The Impact on Middle Management. The potential for strategic use of information technology generates a high level of visibility across the organization in an area in which managing the systems development process is difficult at best. As a result, middle managers in corporate information systems departments and user areas alike are “feeling the heat” more than ever before. For example, timing is everything with these systems. Exactly when a strategic information system is implemented is critical. The sooner that such a system can be made available to the users, the greater the competitive advantage generated.

Executives know this, and senior management’s growing attention in this area increases the pressure on information technology managers, their staffs, and related user departments to produce high quality strategic systems without significant delays.

The Pressure to Succeed. Information technology managers often correctly view participation in such highly visible projects as rare opportunities that can “make or break” a career. Thus, they tend to try to conclude such projects successfully at almost any cost. One unfortunate byproduct of high corporate visibility is the temptation for information technology managers to “throw caution to the wind” in an attempt to get the system working on schedule and within budget. The tendency too often is to take risky shortcuts. In particular, managers can fail to observe adequate safeguards in the hiring and monitoring of individuals responsible for executing the various project tasks assigned by management. Finding and keeping personnel with the right combination of technical skills becomes an overriding concern. Other dimensions, such as honesty and integrity, tend to get lost in the short-term shuffle of day-to-day project management.

ETHICS IN PROGRAMMING
Because of the scarcity of technical computer systems talent, organizations do tend to be lenient with
programmers, thereby implicitly sanctioning improper behaviors that would simply not be tolerated for nontechnical, less essential personnel. Selectively enforcing prohibitions against unethical behavior in this way contributes to the individual programmer’s belief that the organization will not act if the rules are bent a little.

The Question of Professionalism. Gellerman (1989) notes that “to rely exclusively on each individual’s sense of right and wrong is to risk ethical disaster”. Ultimately, the employees’ ethical point of view relates to his or her sense of professionalism. In established professions, such as accounting, medicine, and law, there are codes of professional behavior mandated by state laws and strictly enforced by state licensing agencies. The key point is that without a state license, individuals are legally prohibited from practicing the professions of public accounting, medicine, or law. No similar credentials are needed to “practice” the programming profession.

For programmers, there are no binding codes of ethics or state regulated professional licensing arrangements. There is only the possibility of voluntary compliance with corporate ethical codes and participation in the certification programs of computer-related professional societies. Many computer programmers do not care to join such societies and tend to be unaware of their codes of ethics or the other aspects of professionalism that these societies try to promote. This is not to imply that computer programmers as a group are unethical or unprofessional people. Most are highly professional and ethical individuals. The point is that the degree of professionalism and the ethical orientation of computer programmers cannot be inferred from reference to established objective standards or through reliance upon professional licensing practices. Thus, when it comes to strategic information systems, merely evaluating a programmer’s technical skills is not enough. Executive management must convince itself that the people in key positions dealing with these critical systems are reliable, honest, and trustworthy employees.

The Concept of Intellectual Property. Data organization and computer software are intellectual properties recognized by the courts and legislatures as predictable property interests (Lessig, 1999). It is a basic principle that the companies that pay programmers to develop software-based properties own those properties. Even so, the most technically complete and in-depth understanding of specific software properties tends to remain with the individual programmers who developed the software in the first place.
Being key participants in the “birthing” process for a particular system, it is easy to see how programmers might come to view an application system as rightfully belonging to them. Although this viewpoint is not legally defensible, it serves as a rationalization for what would otherwise be unthinkable conduct by professional programmers. Dishonest, or even disgruntled, systems employees may use this rationalization to help justify their actions to themselves or to other employees who may be consorting with them.

Rights to intellectual property are particularly difficult to enforce. Mason (1986) notes that “One of the most complex issues we face as a society is the question of intellectual property rights.” He summarizes the problem as follows: “Any individual item of information can be extremely costly to produce in the first instance. Yet, once it is produced, that information has the illusive quality of being easy to reproduce and to share with others. Moreover, this replication can take place without destroying the original. This makes information [and the software that manipulates it] hard to safeguard.”

With information systems, employers have recognized the problem of the programmer who does not appreciate the distinction between his own intellectual contribution to developing a system and the intellectual property rights of the employing company. Corporations engaged in technologically-oriented business activities generally require new employees to sign a secrecy agreement specifically designed to protect the employer’s rights to proprietary information, including documents, technology, trade secrets, and even “know—how.” Versions of these kinds of secrecy agreements are constructed to cover the activities of programming and other systems personnel as well.

The Influence of Organizational Factors. Programmers tend to be isolated from the rest of the organization in which they work, making it particularly difficult for programming staff to be exposed to the traditional values of the organization and to gain a sense of allegiance to the corporation. In fact, programmers are known for exhibiting higher loyalty to their individual technical specialties than to their employers. They tend to identify more strongly with their roles as technical experts than with their roles as corporate employees. For these reasons, it is difficult to build a sense of ethical commitment among programmers. Another factor in the ethical make-up of programming professionals has to do with excessively rapid advancement. Rapid promotions can result in programming staff members assuming relatively high levels of responsibility before they have had time to assimilate their employer’s ethical value system.
advancement is typical of computer programming organizations, particularly among programming project leaders. The risk that these technical supervisory personnel might be tempted to sanction unprofessional behavior in areas under their control will be higher if they have not had the opportunity to fully internalize the corporation’s norms and ethical point of view. Another situation occurs when management simply fails to discipline unprofessional conduct. Whenever a bad example is set by the obvious failure to punish employees who have behaved unprofessionally, their peers and subordinates begin to question the organization’s real values. Such cynicism is a particularly difficult problem within the context of computer programming. The demand for skilled programmers is increasing as computing proliferates across business organizations, while the supply of these same skilled programmers is declining. Project managers view programmers’ technical expertise as critical to the short-term success of programming projects. Consequently, it may be safer and easier for the project leader to avoid confrontation and ignore unprofessional behavior when the alternative is to risk losing a key programming resource that will be difficult to replace and may cause a delay in project completion. This supervisory behavior helps to foster a dangerous attitude among programmers that they are not governed by the rules that apply to everyone else in the company. **BOGART - A CASE IN POINT**

The importance of establishing adequate corporate safeguards for strategic information systems in selecting programming staff, in monitoring their work activities, and in making clear that unethical conduct will not be tolerated, is demonstrated in the following case situation. **Overview of the Case.** Late during 1986, two computer programmers, Roy Johnson and Jerry Williams, were employed by Bogart Engineers and Constructors, Inc., of Houston, Texas. (These names are aliases.) These programmers were immediately assigned to a project team dedicated to the development of a critical corporate information system. This system was considered by Bogart management to be strategically crucial to Bogart’s competitive position in its basic market, providing engineering and construction services for the petrochemical industry. The new system was aimed at streamlining Bogart’s engineering design process. The software to be developed by Bogart was similar to other products available in the computer-aided design software marketplace, but was differentiated by two factors that Bogart considered key:

1. The Bogart system provided a wider range of design options than other products then available.
2. The Bogart system provided for the computerized creation of design drawings, eliminating the need for craftsmen in the design of plant facilities for its customers.

Bogart staff could input design criteria and parameters at the end of the work day, leave the computer to
perform designated tasks, and return the next morning with drawings completed. Bogart envisioned that
the new system would catapult Bogart into a competitively powerful position in its primary markets.
As the events of 1987 unfolded, Bogart management became aware that Johnson and Williams had placed
their own ambitions ahead of Bogart’s interests regarding the software that they had developed in spite of
the fact that Bogart was paying them for their work. Furthermore, their actions violated the terms of
confidentiality agreements that each had previously signed which clearly defined Bogart’s proprietary
interest in the product of their work assignments. Civil legal action to protect Bogart’s position began
accordingly in 1987 and was the subject of a complicated settlement agreement filed and sealed in the
Texas courts in 1989.
In addition to the controversy regarding proprietary claims, one of the programmers encoded into the
programs “destruct” mechanisms designed to cause program modules to crash and become worthless at
specific dates and times in the future. This conduct, which was in violation of Texas Penal Statutes,
resulted in prosecution under Texas criminal law protecting computer hardware and software from
unauthorized tampering or destruction.
Bogart’s Competitive Situation. At the time of this case, Bogart Engineers and Constructors, Inc.,
employed nearly nine hundred people in the Houston area. The company was (and is) primarily engaged
in providing engineering, design, and construction services to the process, refining, and petrochemical
industries. Mostly, Bogart designs and builds refineries and chemical plants for major oil companies.
In the 1980’s and 1990’s, Bogart operated in a highly competitive service industry with rivals including
such major companies as Bechtel, Fluor, M.W. Kellogg, and Stone & Webster. Technological innovation
was critical to gaining competitive advantage and also avoiding competitive disadvantage. This industry
was (and is) service-oriented and highly labor intensive. The competitive value of technological advances
that reduced labor costs could not be overemphasized. Labor costs comprised a significant portion of the
costs of services provided by Bogart for most projects undertaken by the company.
Strategic System Concept Identified. In 1986, internal studies conducted by Bogart indicated that Bogart
was losing competitive ground because its project proposals were quoting excessive manhour utilization
levels that compared unfavorably with competitor’s proposals. Bogart discovered that it was in the
position of being a follower in utilizing information systems strategically in this area. As a result, Bogart intensified internal development of program technology to enable the company to reduce manhours needed to complete engineering and construction projects. The software that was eventually developed to accomplish this objective was named the “Bogart Instrument Design System,” or more simply, the “B.I.D. System.”

B.I.D. System Development Project. The B.I.D. System project was a fast track project with bonuses given to programming staff at the completion of each successive project milestone. Project team members were allowed to work at home using personal computers supplied by the company as standalone workstations or as terminals to link to Bogart’s corporate computers, as appropriate. The project team consisted of Johnson, Williams, and two other programmers. In April of 1987, one of the other programmers assigned to the project noticed a microscopic legend inserted as a microdot within the Bogart corporate logo on one of the engineering drawings created by the Bogart system. After examination, it was discovered to the subsequent amazement of the Bogart management team that the microdot stated “Roy Johnson and Jerry Williams, Copyright, 1987”!

Bogart’s Initial Response. After the legend hidden in the microdot was discovered, Bogart executive management was notified. They immediately perceived this situation as a serious business threat. The executives became convinced that Johnson and Williams intended to claim ownership of the software and market it to Bogart’s rivals. Consequently, a new and more restrictive secrecy agreement was developed. All Bogart programmers were asked to sign the new secrecy agreement. Johnson and Williams refused to sign. The following day Johnson reported to work briefly to resign from the company and Williams failed to report to work at all. An immediate investigation of the status of the B.I.D. System at Bogart revealed that the B.I.D. System programs, B.I.D. System documentation, and all of the related data files were missing. A review of the circumstances of the disappearance showed that Williams probably removed the system from the Bogart premises the day before. Subsequently, in a telephone conversation, Williams disclosed that he had the missing software, data, and documentation in his possession. Williams indicated that he would return it upon receipt of his and Johnson’ final paychecks from Bogart. The missing items were returned by Williams later that same day.

Damage to the B.I.D. System. Inspection of the B.I.D. System program modules at that time revealed the following irregularities:

i) All indentations, line spaces, and comment lines had been removed from the B.I.D.
System program modules.

ii) The main B.I.D. System program module had been modified to self-destruct and print “garbage” after a period of ninety days had elapsed.

iii) Each program module had been modified so that it would print a legend on every document created by the system after the same period of ninety days. The legend stated “PROGRAM DEVELOPED BY ROY JOHNSON AND JERRY WILLIAMS, HOUSTON, TEXAS”.

iv) Each program module had been further modified so that after a period of one hundred and twenty days had expired, the B.I.D. System would destroy all of its own output records as they were being created; the system would cease to function.

9

The extensive tampering with the B.I.D. System forced Bogart to dedicate substantial personnel and computing resources to eventually return the program modules to their original form.

Direct Costs of B.I.D. System Recovery. Bogart assigned its most capable technical personnel to correct, rewrite, and debug the compromised program modules. Estimates of the cost of system development prior to discovery of the “software time bombs” were easily in excess of $200,000. Reversing the damage to the system cost at least $50,000; and lost profit due to lost work opportunity directly attributable to the B.I.D. System tampering was estimated in excess of $1,000,000. Fortunately, tampering was discovered well before Johnson and Williams had achieved their malicious intent. Therefore, the loss to Bogart, while not trivial, was substantially less than what would have occurred if Johnson and Williams had succeeded.

Less Tangible Costs of Recovery. The resulting litigation lasted from the Fall of 1987 into the Fall of 1989, absorbing significant senior management time and resources. The litigation proceeded along two basic fronts, civil and criminal. First, in the civil court action, Bogart initially secured an injunction to halt further use or development of the software by Johnson and Williams pending resolution of the case in civil court. Second, the District Attorney obtained a felony indictment of Jerry Williams. During the criminal investigation, Williams consented to a taped confession in which he admitted that he had, in fact, inserted the self-destruct code into the B.I.D. System computer program modules. In November of 1989, Bogart, Johnson, and Williams entered into an agreed judgment containing a permanent injunction offering the protection that Bogart considered essential. Jerry Williams subsequently entered a plea of “guilty” in the criminal proceedings; and the entire episode was finally concluded. In terms of lost business opportunity, expenditures made to recover the B.I.D. System software, non-remunerative
distractions endured by Bogart management, and court costs and legal fees, Bogart paid a high price to
protect its proprietary information systems technology and the associated competitive advantage. Could Bogart have avoided this situation? The following set of recommendations suggests that some, if
not all, of the difficulties encountered could have been avoided through lucid and consistently applied
management policy and strengthened management controls covering protection of strategic information
systems and their application.

**RECOMMENDATIONS FOR EXECUTIVES**

Recommendations Derived from the Bogart Case. A number of measures should be encouraged in any
organization exposed to the potential for tampering or other misfeasance by information systems
employees. These measures are particularly important for situations in which employees are
developing, maintaining, or operating systems that are considered to be strategic. In these situations, the
following recommendations are key:

1. **Avoid Implicit Sanctioning**. Corporate management should send a clear signal throughout
the organization of its policy regarding the handling of misconduct in connection with
use of computer hardware or software. Aggressive enforcement of the policy, such as
occurred in the Bogart case, is key to successful policy implementation.

2. **Use Secrecy Agreements**. Employees should be required to read and to sign an
acknowledgement of the corporation’s intellectual property policy for computer
application systems.

3. **Focus Attention on Strategic Systems**. Corporate management should identify those
computer applications that are strategic in nature and supervise these systems with greater
care and more attention to management detail than with less critical computer
applications.
The following should be the key areas of focus:

   • The assignment of proven, reliable personnel to develop, maintain, and operate
     such strategic systems;
   • The implementation of secure recovery procedures in case of compromise of
     these strategic systems;
   • The frequent review of the status of these strategic systems by organizationally
     independent, technically qualified, and reliable personnel.

4. **Limit Access to Strategic Systems**. Access to computer applications should be limited
only to those having a recognized “need to know” and only upon attaining appropriate
approvals from management. For strategic information systems, these approvals should
be secured from, or at least reviewed and approved by, corporate executive management.

5. **Prepare Employees to Recognize Misconduct**. Training programs dedicated to sensitizing
information systems employees to the symptoms of computer tampering and assisting
these employees in recognizing tampering by other employees should be initiated. Such
training programs will elevate the general awareness of the possibility of unethical
behavior among programming and operating staffs and help to discourage those
individuals who otherwise might consider engaging in such misconduct.

6. **Limit Opportunities for Telecommuting**. Permitting information systems employees to
work at home should not be encouraged unless the employees’ reliability and level of
professionalism is well established. It is more difficult to control employees who work
outside the office. In particular, information systems employees involved with strategic information systems should be discouraged from telecommuting because working at home may invite abuse.

7. Emphasize Quality Assurance of Strategic Information Systems. The quality assurance function within the information systems organization should be required to frequently review the status of information systems development and operation. Strategically important information systems should be identified by quality assurance personnel and reviewed more frequently than similar reviews for non-strategic systems. The quality assurance function should provide for the systematic backup of strategic software levels independent of developmental or operational personnel. In this way, quality assurance can provide a mechanism to restore the functionality of compromised strategic software quickly if computer tampering should occur.

8. Audit Strategic Systems Management Procedures Regularly. An independent information systems audit function outside of the information systems organization should be utilized to periodically evaluate the management procedures employed in the development, maintenance, and operation of strategic information systems. The audit function should examine management practices and determine the degree of compliance with corporate policy for managing information technology. Special attention to assessing compliance for strategic information systems applications should be a priority.

New Reality for Information Technology Managers. These recommendations derive from a new business reality, that the strategic use of information technology for competitive advantage in modern business changes how executives must view and control the information systems function. Each individual organization may have additional requirements for protecting its own strategic information systems depending upon that organization’s information systems environment and implementation approach. Nevertheless, the protective measures outlined above will provide a solid basis for assuring the ongoing integrity of the corporation’s investment in strategic information systems applications. If Bogart Engineers and Constructors, Inc., had followed the recommendations outlined above, Roy Johnson and Jerry Williams would have been far less able to operate unethically and illegally within the company. It is clear that Bogart was lucky, having stumbled onto evidence of two of its employees’ illegal behavior before the employees could carry out their plans fully. Thus, Bogart avoided a potentially devastating loss of a strategically valuable information systems application. Other organizations may not be so fortunate.

REFERENCES
Callahan, C. V., & Pasternack, B. R. Corporate Strategy in the Digital Age. Strategy and Business, 2nd


