Cooperative Extension College of Agriculture Washington State University Pullman, Washington 99164

AGRIBUSINESS MANAGEMENT

TECHIES, JUNKIES, AND HACKERS: COMPUTERS IN THE AGRIBUSINESS INDUSTRY

A recent courtroom experience and a popular magazine article, together, generated the courage to write this piece. The incentive to do so had long been latent. I had suppressed the urge to address the subject out of a combined fear of professional rejection and no small amount of personal insecurity. Computers have long been an acceptable component of academic life. Desktop PCs, portables, mainframes, and their multiple-location linked terminals have become almost as common to campus office surroundings as file cabinets and credenzas. Their use by faculty and graduate students in research activities has grown to a level judged "expensive" by administration and "indispensable" by the researchers themselves. Having once crunched numbers on an old manual calculator during my graduate training, I welcomed the advent of the electronic data processing age. This fact notwithstanding, it was not by accident that computers appeared first on the desks of our secretarial personnel and only much later in the offices of our faculty. Computer proficiency in word processing was the key to this prioritization. Private industry followed a similar pattern as staff (not management) was often the first to gain access to electronic hardware. Staff personnel, therefore, first developed computer use skills, while upper level management remained aloof. Since staff was normally responsible for routine, repetitive, and procedural matters, the adoption of computers was judged logical and, after a period of introduction, they proved highly beneficial to the office place. But as noted, their greatest use was in the performance of routine, repetitive, or data-heavy activities. Once the hardware was in place and procedural programs were written, both speed and efficiency were enhanced. Gradually, however, computers found their way onto the desks of decision makers — those who were responsible for thinking, contemplating, and innovating. And it was at this point that some interesting problems began to arise.

If you will pardon this lengthy introduction, I will now return to my earlier remarks. I recently had an opportunity to observe the court proceedings of a farm bankruptcy. The farmer-petitioner was asked to describe to the court how it was that the farmer had, in the past two years, managed to pay numerous unsecured creditors (suppliers of farm inputs), while the secured creditor (a bank providing long-term real estate financing) had remained unpaid. The farmer answered that input suppliers were very persistent, and demanded payment immediately following harvest. Furthermore, he lamented, he routinely forgot when the real estate payment was due, and when he was reminded, working capital shortages prohibited payment. To further document his good intentions, the farmer proudly explained that he had purchased an expensive computer, whose responsibility it was to regularly remind him of pending debt payment schedules. Each day as he logged on, the software filled the monitor's screen with debt payment due dates. It was, as the farmer explained, "like being reminded that there were only 65 shopping days before Christmas." After a pause and a deeply saddened glance at the judge, the farmer admitted that while the computer had fulfilled its assignment, it alone could not pay the

bills, as cash flow remained short. His final admission, within this rather emotional scene, was that long-term loan payments remained in arrears and he now owed a computer sales/serviceman nearly $5,000! I couldn't help but wonder how often this scene was being repeated throughout the agribusiness industry. Shortly following this experience, I read an article titled "Computer Headaches" in *Newsweek* (July 6, 1987). This article served to further stimulate my concern for those problems which arise when computers are introduced into the offices of business decision makers. As noted in this article, the linkage between a computer keyboard and "the boss" can often become a tenuous and unpredictable one. Under worst case scenarios the computer becomes the surrogate for human judgment, innovative thought, and integrity. So-called techies, junkies, and hackers arise from this situation, and as a result, some businesses falter. Hopefully, the following discussion will better describe these problems and how they might be avoided.

The Computer Junkie

Even those who are least observant would argue that computers have all but revolutionized routine office practices. As I visit agribusiness firms, even the smallest organizations provide ample evidence that computers have automated the "grunt work" such as payroll, records, and accounts. Inventory and monthly billings are also subject to improved proficiencies under electronic data processing. But as is often the case with technological adaptations, for every few steps forward, there is an occasional step backward. In the latter case, the hardware is certainly not to blame. While the computer is normally viewed within a mechanical/electronic mode, I would argue that it also has a cultural impact. In fact, as computers expand from primary use by staff to occasional use by top management, a true cultural change emerges. Agribusiness managers who were in vocal opposition to their need for this new technology find themselves gradually seduced/coerced into a general acceptance. This cultural impact is characterized by the state of embarrassment which arises when "the boss" must seek guidance from his/her secretary to gain a familiarity with introductory software and basic computer procedures. For some managers, this sense of embarrassment is so great that they will return to the office after hours to struggle with their new machines in a state of privacy. Gradually their skills improve to the point where they can come out of the closet and publicly declare their computer literacy.

It is at this stage that the first danger arises. To retain a sense of position, the boss struggles with the perceived need to demonstrate that his/her computer skills have surpassed those of subordinates. Increasing amounts of time are spent before the monitor. Phone calls and routine matters are diverted as the boss begins to experiment with the endless opportunities afforded by the new innovation. Most agribusiness managers will gradually regain their composure and properly assimilate their newly acquired skills into their daily decision-making responsibilities. Others, however, will find they are captured, growing increasingly stimulated by, and dependent upon, their computers. They have become computer junkies, as all aspects of managerial activity are subjected to computer analysis before decisions are rendered. Managerial productivity actually declines as this dependency contributes towards delays, frustrations, and an overly zealous search for data (even trivial or irrelevant data) to enter into the computer. Gradually the manager loses touch with the business as he/she abdicates personal judgment in favor of what the computer says. I have personally witnessed this addiction, finding some managers who physically carry their PCs home and/or travel with them. The need for, and usefulness of, the computer has been exceeded and the business will incur the penalty.

The Computer Techie

"Nerds" have always existed in our society, but only recently have they been recognized as such in our language. Within our youth culture, nerds are identified by dress, attitude, and personality. But our agribusiness culture has also given rise to its own nerds. They are better known as computer techies. As so accurately depicted in the *Newsweek* article, techies pose as much of a threat to themselves as to the office where they work. On their business cards should be emblazoned the words, "I'm computer friendly, just watch me play." Indeed, to the techie, the computer represents a game - a game to be played competitively, with skill and persistence. All else is secondary. All business tasks, no matter how simple and menial, are destined for computer adaptation. Techies take great personal pride in fostering and perpetuating their reputations as computer jocks. They romp gallantly from one terminal to another, de-bugging each program, enhancing others, and generally making a technological nuisance of themselves.

I once discovered such a techie employed in an agribusiness supply operation. He had coded the odometer reading and operator of each of the firm's service vehicles into the computer and daily checks were required to calculate mileage driven and allocate the appropriate costs. So burdensome had this task become that employees had elected to use personal vehicles for company business rather than defend themselves against the scrutiny of the system. Other similar systems had been employed to monitor service calls, gasoline consumption, and telephone usage. As each new system was installed, the techie was playing his game, demonstrating his indispensability, and further alienating his co-workers. Worse yet, management began to believe that this individual was productive and invaluable to the business. Quite the reverse was true, as employees had wasted valuable time inventing devious means for outflanking or trashing the various systems and destroying the validity of the data produced at each month's end. But the true techie is often undaunted in his/her search for a broadening of the gaming possibilities. These nerds of the agribusiness world are little more than "geeks with computer power," and if left unchecked, will diminish rather than enhance company productivity and managerial proficiency.

A slight mutation of the techie is the gamer. So enthralled are these individuals with their electronic abilities that they abandon all linkages with business-source data and launch into independent gaming software. Always willing to titillate the psyche of computer literates, several software manufacturers have created games which managers can play on company time with assurances of never being discovered. I know, because I've committed this venial sin myself. Holding a pilot's license, but lacking the funds to own or rent an airplane, I once purchased a computer program which simulated the experience of piloting a small aircraft under instrument conditions. The game went into my briefcase and off to my office PC almost immediately. When I was stuck with the doldrums of a slow day, my office door was closed and I (figuratively) flew off into some endless cloudbank with my propeller-powered PC. Fully aware of this gaming instinct, the software manufacturer had incorporated into the simulated flight program a so-called "boss button." If there was an unexpected knock on my office door, I only needed to press the "boss button" and the monitor's screen was filled instantly with an impressive-looking financial spread sheet. Oh what miracles has technology wrought? Is such office conduct the exception? Unfortunately not. *Newsweek*, in fact, reported that one survey found that 66% of business executives used their computer for non-business purposes, and of those, well over half admitted playing games on company time. As I stated in the introduction, for every few steps forward, there is one step backward.

The Computer Hacker

The junkie, the techie, and even the gamer are potential problems to the agribusiness industry, but one must admit that none of these represent an intentional or all-threatening difficulty. While the nuisance factor is present in each, and each may detract from productivity and managerial proficiency, none is singularly intent on destruction of the business. Occasionally, however, the junkie, the techie, and the gamer may cross the boundary between the benign and the illicit. When computer aficionados intentionally cross over that boundary, they have entered the world of the abusive hacker. Hackers are defined as those persons, internal or external to the organization, who illicitly breach a firm's computer security for purposes of personal exploitation or gain. It is a silent form of criminal conduct — often unnoticed, largely unsuspected, and rarely publicized. Yet it does exist and must be addressed.

In a survey recently released by the accounting firm of Coopers and Lybrand, 10% of insurance companies reportedly discovered breaches to their computer security systems and 90% of those reported altered data, destroyed data, or embezzled data. There are obvious reasons why such discoveries are not widely known. Most of us would wonder why a small agribusiness firm would ever be subject to such criminal action. In fact, few are. But while such businesses are less attractive or susceptible than larger financial complexes, they cannot dismiss the threat. All businesses, no matter how simple or small, generate and seek to retain and protect confidential data. To the extent that computer systems provide the storage medium for such data, illicit access and use remains of concern. In the era of the file cabinet, most agribusiness firms followed some basic program for securing their storage. Converting to a computer-based records system, however, caused some to lower their guard. The reverse should have been true, however, because criminal access to the computer files no longer required a physical presence. Electronic access was now possible from distant locations, access was instantaneous, and the illicit search was actually aided by the system itself. Hackers, therefore, are the most proficient of all criminals. They access records from a distant location, leave behind few clues of their actions, and selectively seek, copy, or destroy data with the speed of an electrical impulse.

Hackers, however, remain a distant threat. In 20 years of experience with the agribusiness industry, I can recall only two occasions where records were altered or destroyed, presumably with intent. But as computers continue to fulfill more critical functions within the industry, the industry must also establish a security network commensurate with that role. I suspect that a cursory review of your current data base would unveil a stock of confidential information larger than you might envision. Protect it as you would all other aspects of your business.

Remedial Measures

In 1986, a study by Kepner-Tregoe, Inc., revealed that 64% of the top executives of Fortune 500 companies never used a computer. Many agribusiness executives continue to harbor suspicions and misconceptions regarding computer capabilities and capacities.

A certain level of distrust can even be found amongst certain groups of agribusiness managers. But, gradually a transformation is occurring and while computers were first used to perform routine and menial tasks, they are now beginning to appear on the desks of some top managers and decision makers. This trend has both positive and negative implications. On the positive side, it means that computers are slowly being accepted by top industry people. Their future use, both for routine and innovative tasks, is growing more secure. On the negative side, however, computers in management will likely give rise to personifications that may

adversely impact the firm if remedial measures are not taken.

If your organization contributes toward the creation of a computer junkie, quick action is required. Their addiction is rendered more acute by a perceived sense of their own importance to the firm. They create computer fiefdoms within which they can run with reckless abandon away from the practical needs of the firm for their services. If left unchecked, they pupate into so-called "big-iron bigots" who capture and control mainframes, whereby access is selectively controlled. Management must trash any system that fosters or perpetuates the junkie. Computers must be recognized for what they can, and cannot, do. Computer operators should not be considered for industrial canonization. They must not be allowed to ascend to heights not supported by the practical value of their true contribution.

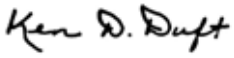
Some combination of a classroom nerd and a computer jock gives rise to the so-called computer techie. To the techie, the computer, itself, becomes the all-encompassing objective. Data and practical business problems merely provide the base upon which the gaming mode is exercised. The techie devotes his/her energy, talent, and enthusiasm exclusively to the computer; all else is seemingly mundane. The secret here is to redirect that talent and energy into something of value to the agribusiness firm.

Convince that techie that he/she is an important member of a total team effort. If their individual effort does not contribute towards the team's objective, such effort will be judged less productive. Never allow the techie to run with a free rein in your business. Channel and focus their work towards the creation of computer systems which enhance rather than detract from the productivity of co-workers.

The computer hacker represents a problem of more serious dimensions. A reasonable computer security system with back-up permanent storage is generally adequate for agribusiness firms. Good, solid financial audits will also provide some protection from all but the thoroughly skilled and unscrupulous. A modest amount of caution is always advisable.

I wish you well with your computer systems. Agribusiness managers should not fear their adoption. Use them wisely and prudently, but exercise those cautions which discourage creation of junkies, techies, and hackers.

Sincerely,



Ken D. Duft
Extension Marketing Economist