SECURITY

10 ethical issues confronting IT managers

Should employees be told to what extent their behavior is monitored? How much effort and expense should managers incur in considering questions of data access and privacy? Does the availability of information justify its use? CIO Jeff Relkin examines these and other ethical concerns facing today's IT manager.

By Guest Contributor I August 15, 2006,12:00 AM PST

By Jeff Relkin

In "10 ethical issues raised by IT capabilities," (http://www.techrepublic.com/5100-10878-6091121.html) we examined ethical issues raised by IT capabilities, issues that all of us as technology professionals need to consider as we go about our duties. This time, we take a look at ethical issues more specific to management-and not necessarily just IT management. Once again, one of our themes is that advances in technology, just like advances in any other area of endeavor, can generate societal changes that should cause us to reexamine our behavior. The dynamic nature of civilization means some components of ethical codes that were perfectly appropriate in previous generations may no longer apply. Although space limits us to 10 issues, the ones we examine here are based on five main categories of particular interest to technologists: privacy, ownership, control, accuracy, and security. As in the previous article there are more questions than answers.

#1: PRIVACY: Does information's availability justify its use?

Governments collect massive amounts of data on individuals and organizations and use it for a variety of purposes: national security, accurate tax collection, demographics, international geopolitical strategic analysis, etc. Corporations do the same for commercial reasons; to increase business, control expense, enhance profitability, gain market share, etc. Technological advances in both hardware and software have significantly changed the scope of what can be amassed and processed. Massive quantities of data, measured in petabytes and beyond, can be centrally stored and retrieved effortlessly and quickly. Seemingly disparate sources of data can be cross-referenced to glean new meanings when one set of data is viewed within the context of another.

In the 1930s and 1940s the volumes of data available were miniscule by comparison and the "processing" of that data was entirely manual. Had even a small portion of today's capabilities existed, the world as we now know it would probably be quite different.

Should organizations' ability to collect and process data on exponentially increasing scales be limited in any way? Does the fact that information can be architected for a particular purpose mean it should be, even if by so doing individual privacy rights are potentially violated? If data meant for one use is diverted to another process which is socially redeeming and would result in a greater good or could result in a financial gain, does that mitigate the ethical dilemma, no matter how innocent and pure the motivation?

#2: PRIVACY: How much effort and expense should managers incur in considering questions of data access and privacy?

This is an issue with both internal and external implications. All organizations collect personal data on employees, data that if not properly safeguarded can result in significant negative implications for individuals. Information such as compensation and background data and personal identification information, such as social security number and account identifiers, all have to be maintained and accessed by authorized personnel. Systems that track this data can be secured, but at some point data must leave those systems and be used. Operational policies and procedures can address the proper handling of that data but if they're not followed or enforced, there's hardly any point in having them. Organizations routinely share data with each other, merging databases containing all kinds of identifiers.

What's the extent of the responsibility we should expect from the stewards of this data? Since there's no perfect solution, where's the tipping point beyond which efforts to ensure data can be accessed only by those who are authorized to do so can be considered reasonable and appropriate?

#3: OWNERSHIP: What can employers expect from employees with regard to nondisclosure when going to work for another firm?

Many people are required to sign NDAs (nondisclosure agreements) and noncompete clauses in employment contracts, legal documents that restrict their ability to share information with other future employers even to the point of disallowing them to join certain companies or continue to participate in a particular industry.

What about the rest of us, who have no such legal restrictions? In the course of our work for employer A, we are privy to trade secrets, internal documents, proprietary processes and technology, and other information creating competitive advantage. We can't do a brain dump when we leave to go to work for employer B: we carry that information with us. Is it ethical to use our special knowledge gained at one employer to the benefit of another? How do you realistically restrict yourself from doing so?

#4: OWNERSHIP: What part of an information asset belongs to an organization and what is simply part of an employee's general knowledge?

Information, knowledge, and skills we develop in the course of working on projects can be inextricably intertwined. You're the project manager for an effort to reengineer your company's marketing operations system. You have access to confidential internal memoranda on key organization strategic and procedural information. To build the new system, you and your team have to go for some advanced technical training on the new technology products you'll be using. The new system you build is completely revolutionary in design and execution.

Although there are areas of patent law that cover many such situations, there’s not much in the way of case law testing this just yet, and of course laws vary between countries. Clearly, you've built an asset owned by your company, but do you have a legitimate claim to any part of it? Can you take any part of this knowledge or even the design or code itself with you to another employer or for the purpose of starting your own company? Suppose you do strike

out on your own and sell your system to other companies. Is the ethical dilemma mitigated by the fact that your original company isn't in the software business? Or that you've sold your product only to noncompeting companies? What if we were talking about a database instead of a system?

#5: CONTROL: Do employees know the degree to which behavior is monitored?

Organizations have the right to monitor what employees do (management is measurement) and how technology systems are used. It's common practice to notify employees that when they use organizational assets such as networks or Internet access, they should have no expectation of privacy. Even without that disclaimer, they really don't need the warning to know this monitoring is, or could be, taking place.

Do organizations have an obligation to notify employees as to the extent of that monitoring? Should an organization make it clear that in addition to monitoring how long employees are using the Internet, it's also watching which Web sites they visit? If the organization merely says there's no expectation of privacy when using the e-mail system, is it an ethical violation when employees later find out it was actually reading their e-mails?

#6: CONTROL: Does data gathered violate employee privacy rights?

Many organizations have started adding a credit and background check to the standard reference check during the hiring process. Are those organizations obligated to tell us they're doing this and what results they've received? The justification for doing the credit check typically is that a person who can't manage his or her own finances probably can't be trusted with any fiduciary responsibility on behalf of the organization. Does this pass the smell test or is this actually an infringement of privacy?

Performing these checks is a relatively recent phenomenon, brought on in part by the desire of organizations to protect themselves in the wake of the numerous corporate scandals of the past few years but also because technology has enabled this data to be gathered, processed, and accessed quickly and inexpensively. Is technology responsible for enabling unethical behavior?

#7: ACCURACY: Is accuracy an explicit part of someone's responsibility?

Business has always had a love/hate relationship with accuracy. Effective decision making is driven by accurate information, but quality control comes with a cost both in terms of dollars and productivity. {If you're checking, you can't also be doing.)

In a bygone era, there was less data to work with, and the only quality assurance that needed to be performed was on data...operations and procedures were manual, so it was the output of those functions that was most critical. Technology has enabled vastly more complicated and interconnected processes, such that a problem far upstream in a process has a ripple effect on the rest of the process. Sarbanes Oxley requires the certification of all internal controls in large part for this reason. Unfortunately, accuracy is one of those areas that always seems to be assigned to the dreaded "someone," which all too often translates to no one. On what basis should the level of accuracy in any given system be determined? How much accuracy is sufficient? How should responsibility for accuracy be assigned?

#8: ACCURACY: Have the implications of potential error been anticipated?

Most assembly lines have a cord or chain that can be pulled when a worker notices a particular unit has a flaw. The line is brought to a halt and the unit can either be removed or repaired. The effect of the error can be contained. As complex interactions between systems and ever larger databases have been created, the downstream consequence of error has become vastly more magnified. So too has the growing dependence on highly distributed systems increased the potential for, and the cost of, error.

Do managers have a correspondingly greater responsibility to assess negative outcomes and the mitigations of costs and effects of errors? Can management or system owners be held accountable if unforeseen errors occur? Is this also the case for predictable but unmitigated error?

#9: SECURITY: Have systems been reviewed for the most likely sources of security breach?

As we mentioned in the previous article on ethics, security used to be confined to locking the door on the way out of the office or making sure the lock on the safe was spun to fully engage the tumblers. Technology presents us with a whole new set of security challenges.

Networks can be breached, personal identification information can be compromised, identities can be stolen and potentially result in personal financial ruin, critical confidential corporate information or classified government secrets can be stolen from online systems, Web sites can be hacked, keystroke loggers can be surreptitiously installed, and a host of others. (It's interesting to note at this point that statistics still show that more than 80 percent of stolen data is the result of low tech "dumpster diving," and approximately the same percentage of organizational crime is the result of an inside job.)

How far can-and should-management go in determining the security risks inherent in systems? What level of addressing those risks can be considered reasonable?

#10: SECURITY: What's the liability exposure of managers and the organization?

Can system owners be held personally liable when security is compromised? When an organization holds stewardship of data on external entities-customers, individuals, other organizations-and that data is compromised, to what extent is the victimized corporation liable to the secondary victims, those whose data was stolen?

Organizations generally have internal policies for dealing with security breaches, but not many yet have specific policies to address this area. Managers who do not secure the systems for which they're responsible, employees who cavalierly use information to which they should not have access, and system users who find shortcuts around established security procedures are dealt with in the same fashion as anyone who doesn't meet the fundamental job requirements, anything from transfer or demotion to termination. Should compromised or ineffective security be held to a higher standard?

Jeff Relkin (http://www.techrepublic.com/5213-6257-0.html?id=4497386&redirectTo=%2f7320-22-20.html) has 30+ years of technology-based experience at several Fortune 500 corporations as a developer, consultant, and manager. He has also been an adjunct professor in the master's program at Manhattanville College. At present, he's the CIO of the Millennium Challenge Corporation (MCC), a federal government agency located in Washington, DC. The views expressed in this article do not necessarily represent the views of MCC or the United States of America.