CHAPTER 1

An Introduction to Information Protection and Employee Behavior

In most organizations, information flows at the heart of workplace activities. The effective management of information requires information technology, and that technology is therefore crucial to organizational success. Information technology comes in many forms—networked personal computers, personal productivity devices, software applications, the Internet, and more—but one thing all types of information technology have in common is that their effective use depends upon human users. People put the technology to work in managing information, and people are ultimately responsible for whether information technology succeeds or fails. Within organizations, these people are the employees who use the technology to get their jobs done, serve the needs of customers, and keep the organization running.

Almost all organizations that use information technology in any substantial way are also struggling to maintain effective information security. In an increasing number of organizations, information is among the most valuable assets they possess. As connectivity among information systems has increased, so has the likelihood of intrusion into the systems, thefts of business information, fraudulent use of information, defacement of organizational Web sites, and other forms of information loss or damage. A worldwide army of hackers, virus writers, and scam artists stands poised to inflict as much damage as possible on the Internet-connected organization. Organizations are always vulnerable to these external security threats to some degree, but industry research by Ernst and Young (2002) suggests that many expensive security breaches in fact result from activity that occurs within organizations: the so-called insider threat posed by employees or contractors who possess trusted access to the

company's information and technology. At the low end, losses from security breaches of all types have been estimated at approximately $20 billion per year (counting U.S. organizations only; Security Wire Digest, 2000). Such losses cause organizations to open their wallets: According to a 2002 industry survey by *Information Security* magazine, very large organizations spend an average of $6 million per year on information security measures; smaller ones spend nearly 20 percent of their overall information technology budgets on security.

Among the various security technologies used in organizations, many provide the means to monitor employee behavior. Organizations deploy these complex and expensive monitoring technologies under the belief that secure management of an organization's information assets depends in part upon the behavior of employees. Employees are the "end-users" of much of the organization's information, and that information is very literally at their disposal. When employees are careful to handle information in a secure way, the organization, its customers, and its shareholders benefit from the protection of this key asset. Alternatively, mismanagement of information or the malfeasance of isolated individuals who "go bad" may have devastating effects on the organization's success.

Organizations possess an increasingly powerful technological toolbox for finding out what people are doing on their computers and on the network. For the many employees who use computers, a detailed electronic trail of communications, software utilization, and network activity now fills the log files of company servers. Almost every organization with business processes that connect it to the Internet uses one type of system or another to assess networked computer usage, track network access, warn about inappropriate behavior on the network, or try to ensure that such behavior cannot occur. Software and hardware vendors provide a huge array of options for collecting, storing, analyzing, and generating reports based on telecommunications records, logs of Web usage, addresses of e-mail recipients, and e-mail message content. A plethora of details about employees' work habits, computer usage, and personal demographics, and a wide range of other potentially sensitive information is collected and stored in organizational information systems. Enterprise computing systems contain centralized work records and other information about job-related activities in huge interlinked databases. Camera surveillance has also become increasingly common, particularly in the public spaces of the organization (e.g., lobbies, parking

lots, customer areas of retail stores), but additionally in non-public spaces such as employee break rooms. Smart cards and proximity badges help the organization know where employees are located and what facilities they have used. All of these forms of monitoring and surveillance allow organizations to increase the visibility of employee behavior, analyze typical usage patterns, flag unusual or unauthorized activities, and reduce the lag between the discovery of problems and subsequent action or decision making. Monitoring and surveillance technologies seem to provide a panacea of observation, analysis, prediction, and control for those who wish to reduce the uncertainty, unpredictability, and risks related to the behavior of information systems users.

A series of U.S. industry surveys has shown that employee monitoring and surveillance occur to some degree in the majority of U.S. work organizations (9 to 5, 1990; Orthmann, 1998; Society for Human Resource Management, 1991, 1999, 2001). In their 2004 survey on workplace e-mail and instant messaging, the American Management Association and the ePolicy Institute found that 60 percent of organizations they contacted used software to monitor employees' e-mail correspondence with parties outside the firm (American Management Association & ePolicy Institute, 2004). Although regulatory controls on monitoring and surveillance are sometimes stricter in other locales, such as Canada, Western Europe, Japan, and Australia, the use of electronic monitoring and surveillance of workers and workgroups occurs in those places as well (International Labour Office, 1993; Mayer-Schönberger, 1999). Employee monitoring and surveillance in emergent industrial economies such as India and China also appear to be widespread, but definitive figures from these countries are more difficult to obtain.

On the surface, these varied capabilities for observation and tracking of employee behavior seem to open up a Pandora's box of potential privacy violations, but using the emotionally loaded word "violation" clouds the subtleties involved in the control over information assets in the organization. Managers have always sought strategies for controlling the environments surrounding their organizations and reducing the risks to which their organizations are exposed. Haggerty and Ericson (2000) referred to these concerns as based on management's "desires for control, governance, security, [and] profit ..." (p. 609). Among various methods to impose control on unruly environments, technology has often played a substantial role

(e.g., Simon, 1965, p. 73). Technology stabilizes business processes and makes them more routine. More pointedly, information technology streamlines and amplifies the collection and analysis of data and its use in decision making. Good managerial decisions, in turn, provide the foundation on which successful and sustainable businesses are built.

In opposition to this view, however, privacy advocates and other critics discuss how monitoring and surveillance violates societal norms, cultural preferences, and fundamental personal rights of workers. These critics suggest that with the tacit or explicit approval of regulatory bodies, organizations routinely overstep their bounds by capturing too much information about employees, too frequently, and with too little control over how the data are used, protected, or maintained. The evidence that critics cite arises from a variety of U.S. legal cases—the majority of which have typically been won or settled in the organization's favor—as well as union grievances and popular reports of notable individual cases. These lawsuits arise from aggrieved employees who have been fired or who feel they have suffered some other injustice in the workplace as a result of inaccurate or inappropriate information that has been gathered about them or as a result of information being used in unfair ways. A related danger lies in potential damage to management-labor relationships: In 1987, the U.S. Congress Office of Technology Assessment (OTA) released a report documenting the opposition of 21 national labor unions to the use of computer technology to monitor worker performance (U.S. Congress OTA, 1987, p. 86). Employee privacy is one of its major concerns; few would disagree that it is highly difficult to make any long-lasting or ironclad guarantees about the privacy of confidential data collected by organizations. All of these issues have been used by critics to argue against the extensive use of surveillance and monitoring technologies.

In the present book, we take neither the side of the technologists nor the side of the privacy advocates. Each of their perspectives may have validity in different contexts, but making this issue either black or white passes over a lot of gray territory by assuming that employees simply accept these technologies as deployed; that information technology professionals administer them exactly according to managerial edicts; that relationships among employees, managers, and technologists are either irrelevant or unchanging; and that organizations either impose monitoring, surveillance, and security

technologies in one monolithic, unilateral step or not at all. In reality, we know from research that integrating any type of new technological capability into a firm requires lots of formal and informal negotiations among the different parties involved: managers, employees, information technology professionals, and others (e.g., Davis, 1989). Every group has a different stake in the issues, and we want to ask whether those stakes are ever put down into common ground. It may be that in some organizations a process occurs in which employees, information technology personnel, and managers weigh what valuable information can and should be captured, what the benefits might be for the different parties involved and for the organization as a whole, and what alternative options are available for simultaneously ensuring information security and protecting employees' interests. In other organizations, managers, employees, and information technology people may simply stumble along, reactively implementing technologies in response to one perceived information protection crisis after another, with no clear vision of how the consequences of their decisions about security and privacy will unfold.

With *The Visible Employee*, we take the view that many people in organizations recognize that information is a highly valuable commodity: Thoughtful managers, information technology professionals, and employees function as "intuitive information economists" and work diligently in their own spheres to collect, control, and organize the information at hand. One important kind of information pertains to what people are doing on the network, minute by minute, hour by hour, day by day. Few would disagree that controlling the flow of information about one's own computer activities or those of other people is useful, but how one achieves that control probably depends a lot upon where one stands in the organization. More powerful people have one way of controlling things, while the less powerful have other ways. Personal assets, such as expertise, social relationships, and social exchange, may determine who can learn what, when, and at what cost. Expertise is an increasingly important asset because the sheer complexity of organizational information systems has catapulted information technology professionals upward with respect to the control and influence that they have over organizational processes. Information technologists are therefore taking on a new role in organizations as behavioral observers, analyzers, and even sometimes enforcers. In many organizations, information security specialists and other information technology personnel occupy the

driver's seat of employee monitoring and surveillance technologies. This alteration of the traditional organizational hierarchy complicates the standard tug-of-war between labor and management by creating a new three-way relationship among employee end-users, information technology/security professionals, and managers.

Note that we use this three-way classification of job functions throughout the book with the knowledge that it simplifies (and perhaps even oversimplifies) the politics and roles in many organizations. Yet, as you will see when we present our interview and survey data, this three-way classification seems like a workable simplification by virtue of the consistency in attitudes and beliefs among many members within each group. Even though certain individuals in some organizations may simultaneously live all three roles—for instance, an assistant director of information technology may have deep knowledge of technology and limited executive power but may also feel like just another worker in the context of the larger organization—we believe that the bulk of the members of any sizeable organization think and act most of the time in accordance with one of the three roles. In short, managers manage, technologists control technology, and workers get things done. Members of each group may have a different take on security, privacy, and monitoring based on what they each need to do to survive and thrive in their respective jobs.

Given the likelihood of different perspectives among the three groups, we think it is reasonable to wonder whether they can all see eye to eye on the question of how to maintain security within the organization while respecting the rights and preferences of those whose behavior is monitored in fulfillment of this goal. We believe that it may be possible and feasible for organizations to navigate between the Scylla and Charybdis of information insecurity and employee mistrust. Organizations can have success with both information security and labor relations through careful, simultaneous attention to issues of employee privacy and autonomy, clear communication of organizational policies, and a thoughtful, multiparty approach to information system design. Such efforts will likely require an unprecedented degree of cooperation and integration among managers, human resources staff, information systems professionals, and other functions within organizations. Although such cooperation may be difficult to achieve, we hope that *The Visible Employee* will make cooperation both more feasible and more likely by illuminating the separate perspectives for the benefit of the whole

organization. By documenting and analyzing the relevant information protection problems from perspectives that encompasses managerial, employee, and technological concerns, we expect to describe a middle road that leads toward secure organizational information while also respecting and protecting fundamental employee rights and expected employee privileges. The data we have collected and that we report in this book can inform both future research and humane practice in organizations.

The development of a perspective that simultaneously considers privacy, social dynamics, and technological capability may also provide a useful starting point for further research in monitoring and surveillance. Privacy, in particular, though extensively studied as a legal and philosophical concept (e.g., Garrett, 1974; Gavison, 1980), is a messy area that social scientists are still trying to figure out (e.g., Newell, 1995). From a practical perspective, we believe that evidence of employee resistance to organizational deployment of information technology systems underscores the point that the introduction of monitoring and/or surveillance into an organization is likely to work best after a set of negotiation processes that bring management, employees, and information technologists to the same table. With recognition of and attention to the social dynamics surrounding new information technology by all involved, it is possible to envision effective and beneficial use of organizational monitoring and surveillance to maintain information security.

We refer to our overall approach to conducting research on employees, security, and monitoring as "behavioral information security." In exploring behavioral information security we are trying to understand the nature and origins of security-related behaviors in organizations and use this understanding as a basis for providing practical and principled approaches for increasing information security while respecting employee rights and preferences. We believe that situational factors in the organization interact with personal characteristics of employees to facilitate or inhibit appropriate information security behaviors. In our view, monitoring and surveillance techniques implemented by organizations are one of the most powerful situational factors, but the deployment of these techniques may not always lead to the outcomes that organizational managers anticipated.

The remainder of the book explores these ideas in three major sections. In the first section, Chapters 2, 3, and 4 provide a context and

orientation behind the relevant research work we have conducted in organizations over the past four years. Chapter 2 outlines the array of information security problems faced by organizations and the involvement of employees in both the causation of these problems and the prevention of them. Chapter 3 provides a non-technical introduction and review of the information technology and techniques used in information security in general, as well as more specifically in surveillance and monitoring of employees. Chapter 4 provides a straightforward description of the psychological basis of privacy, along with supporting comments relating privacy to a few of the critical societal and legal issues.

In the middle section, we provide an overview and analysis of the data from our research program. We organize this section based on the perspectives of different groups of people. Chapter 5 describes interviews and other data obtained from managers about monitoring, surveillance, and the role of information security in the organization. Chapter 6 describes data collected by interviewing information security specialists and other information technology professionals with an interest in user behavior. Finally, Chapter 7 describes the employee perspective—including interviews and surveys conducted and observations we have gathered across many different organizations. In each of these chapters, we provide extensive quotes from organizational members with whom we spoke in order to convey the authentic voices of people who have direct concerns and responsibilities for information protection in their organizations. Their thoughts provide a rich picture of the challenges, problems, successes, and failures that contemporary organizations face as they tackle the complex problems of information protection.

In the third and last section, we close by providing reflection, discussion, and recommendations based on our data. In Chapter 8, we provide an integrated perspective on the work we have conducted with one eye on future research directions and perspectives. In Chapter 9, we provide research-based recommendations for managers, human resource professionals, employees, and information security specialists that we hope will lead toward more effective organizational policies and practices in organizations that use information technology. We have also provided a series of appendices, which focus on two separate issues. First, we provide some additional information that shows how we collected our data and what we found. Second, we provide some resources—such as model policies—that

we believe may be helpful as organizations move toward more effective structuring of their measures to protect privacy and maintain security. Teachers and students should note that Appendix A lists supplemental readings for major topics we have covered and Appendix B contains discussion questions pertaining to each chapter of the book.

A Note About Terminology

We have attempted to make *The Visible Employee* comprehensible to a non-technical audience, to those with a modest grasp of information technology, to students in technology and social science programs, and to others with an interest in organizations and information but limited exposure to security concepts. We have tried to minimize use of acronyms, jargon, and specific brand or model names of products in an effort to make the book as reader-friendly as possible. As a result of our trying to thread this needle, some hard-core technology people may find our descriptions of security technologies rather simplistic, and some social scientists may consider our descriptions and analyses of data long-winded and pedantic. All we can ask is that you bear with us and feel free to skim over the parts that seem too elementary. In the material that follows, we provide a few explanations of terminology in advance that may save some problems later.

First, as previously discussed, we have made a tripartite division of organizational roles. When we refer to "managers," we mean all of the people from the executive suite down to the middle management level who have the power and discretion to make decisions, set policy, and spend money. In general, we do not include in this category frontline supervisors or professional employees, even though people in these groups may have some limited spending power and some staff under their control. When we refer to information technology people, information security people, technology experts, and technologists, we are including all individuals in the organization who have responsibilities for some aspect of the organization's information technology infrastructure. Finally, everyone who is not a manager or technology person we call an employee or worker. Collectively, we sometime refer to employees who use information systems as the "user community." We acknowledge that managers

and technologists themselves have the same legal employee status as other workers and that they, too, use information systems, but we split the organization into these three groups in order to analyze and understand what makes their information protection roles different from one another.

We use the phrase "information protection" as an umbrella term to cover any and all efforts to maintain information security as well as the privacy or confidentiality of sensitive information. We define "information security" as the range of technical and social approaches to keeping information confidential, integral, and available (more on this in Chapter 3). We use the term "privacy" to refer more specifically to the control of sensitive information about people (more on this in Chapter 4). In our estimation, organizations cannot protect privacy of employees, customers, or others without a good information security program. For organizations with solid technical information security protections, however, it is still possible to have problems with privacy that adversely affect people. This is because privacy is a human construction—a personal process of controlling information about the self—and the technical security controls that assure the safe flow and storage of data cannot ensure that someone does not become offended or harmed by the way this data is collected, handled, or distributed. Thus, information protection encompasses both security and privacy. As the rest of this book shows, mastery of both the technical and social dimensions is necessary for effective information protection.