December 2006

The Visible Employee: Electronic Monitoring and Information Security

Jeffrey Stanton
Syracuse University School of Information Studies

Kathryn Stam
SUNY Institute of Technology

The Visible Employee: Electronic Monitoring and Information Security

Jeffrey M. Stanton
Syracuse University School of Information Studies
jmstanto@syr.edu

Kathryn R. Stam
SUNY Institute of Technology
stamk@sunyit.edu

ABSTRACT

Every organization creates and processes information in some form. Unfortunately, security threats affecting the organization's information have grown over recent years. Although good technology is critical to information security, user behavior also affects security. Monitoring, surveillance, filtering, logging, and tracking are all words that have been used to describe the processes that organizations use to help understand if, when, and how workers are doing their jobs and handling the organization's data carefully. In this paper, we have distilled key elements of our forthcoming book on this topic. Because of space limitations only 16 interviews are excerpted from the large body of source material we collected. After presenting a summary of these data, we conclude with a preview of recommended processes for supporting information protection that may benefit organizations.

Keywords

Information security, organizational behavior, electronic monitoring.

INTRODUCTION

Technology experts have focused their talents on improving information protection in organizations, and their efforts have led to many effective technical solutions. Few of these solutions focus on the human element in information protection, however, and in particular on the effects of organizational behavior on information security. When workers handle the organization's data inappropriately, everyone and everything around the organization may suffer as a result of lost productivity, lost revenue, legal liability, and financial disaster. Because of the importance of the worker role, organizations go to great lengths to ensure that workers handle information securely. Just as IT facilitates the handling and processing of information, it also facilitates watching those who handle the information at work. Monitoring, surveillance, filtering, logging, and tracking are all words that have been used to describe the processes that organizations use to help understand if, when, and how workers are doing their jobs and handling the organization's lifeblood carefully.

Although some researchers have considered the role of monitoring as a tool in service of security (e.g., Dhillon, 2001; Straub & Nance, 1990), to date few have attempted to integrate the large social science literature on monitoring (e.g., Stanton, 2000) and a psychological perspective on privacy in organizations (e.g., Stanton, 2002), with a practice orientation toward information security governance. In this paper, we have adapted and distilled elements of a book length report covering four years of research that we have described fully in Stanton and Stam (2006). In this paper, we provide an overview of how electronic monitoring and other techniques are used in the pursuit of information protection and what managers, employees, and information technologists think of these techniques. The source material for this research comprised on-site security assessments at 15 small and medium-sized companies, interviews with 75 respondents at those companies, and national (U.S.) surveys with a total of N=1606 research participants, the majority of whom were end users. In this paper we report excerpted material from 16 of the interviews we conducted to illustrate key points, but also provide an overview of the full range of material reported in the book.

HOW MONITORING AND SURVEILLANCE SUPPORT INFORMATION SECURITY

Computer monitoring begins as soon the employee authenticates into a system. Following authentication, network operating systems ensure that each time a user retrieves, modifies, or deletes a file or database entry, a record is made. Although these techniques are useful for monitoring access to local data resources, many companies are equally concerned about their employees' Internet use. Companies may record sender and recipient addresses or keep records of the contents of messages for legal or regulatory purposes. The Enron scandal was marked by public dissemination of a huge email archive, along with concomitant embarrassment by workers who communicated personal information to friends, family members, and each other.

Web tracking and filtering programs stand between each worker's computer and the Internet at large. One security consultant we spoke with in our research said that when he installed web tracking at small- to medium-sized companies he routinely found that the majority of the bandwidth was used for non-business uses of the Internet such as shopping, reading the news, downloading music, and examining pornography. Another company we researched restricted access to non-business sites except between 12:00pm and 12:30pm, during which time workers could browse anything except pornography. A more surreptitious strategy involves no overt restrictions, but instead tallies visits to prohibited sites and raises a flag if a user goes over a preset limit.

Besides looking at Internet activity, however, companies may use more generalized strategies to discover what a worker is doing with his or her computer. Keyloggers, for example, are a favorite tool for internal investigations because they yield a rich stream of information about employees' activities. Because the user is generally unaware of the use of a keylogger on his or her system, the potential for abuse is substantial. Screen capture takes a different approach to finding out what users are doing by periodically copying the entire contents of the computer's display. Because screen shots are not as useful for recording user behavior over long periods of time, some companies also use application usage tracking systems.

Note that it has become common for monitoring and surveillance systems to include most of these features in the same basic package with centralized administration, independent control over the various features and data collection techniques, and sophisticated reporting functions. Lastly, note that some of these systems are inexpensive; the biggest cost is usually ongoing system administration and data analysis.

Non-Computer Surveillance

Beyond monitoring computer use, many possibilities also exist for automated surveillance of workers' non-computer behavior. New digital video capabilities – in particular, motion tracking and biometric identification – have enhanced camera surveillance. Whereas in the past a human would have to scan a surveillance tape, the latest algorithms for facial and gait recognition have ever-improving capabilities for automatically identifying targets. Camera surveillance also has other applications that may become more widespread as concerns about "insider threats" continue. It is now feasible to provide surveillance as a novel form of biometric authentication. Unlike other biometrics, however, digital camera surveillance can continue throughout the user's whole session. Proximity cards also make identification pervasive, because no action by the worker is needed. Such surveillance also makes possible correlated analysis of certain activities such as sending a sensitive document to a printer. Although these capabilities are not likely to become common at most companies, one organization we visited for our research did have similar capabilities to those described above.

Summary

Reflecting back over the description above may provoke a variety of reactions. One reaction may be to think that we have painted a paranoid picture about how monitoring is being used in the service of information security. Although we acknowledge that it is easy to fall into this mindset, we also know that there are many legitimate uses. By showing the capabilities and power of these technologies, however, we also highlight two pitfalls. The first, "mission creep," can gradually or abruptly turn legitimate monitoring into surveillance. The other pitfall pertains to the responsibilities that these technologies put on IT staff members for meticulous care of monitoring data. Mishandling and misuse of monitoring data seem like inevitabilities, unless IT staff members receive the training, support, and supervision they are due when entrusted with these masses of sensitive data.

BELIEFS OF MANAGERS, TECHNOLOGISTS, AND EMPLOYEES ABOUT MONITORING

Below, we report interview responses of non-technical managers (five interviews are excerpted here). Although the managers we interviewed described various approaches for justifying, developing, and communicating policies related to monitoring, there was universal belief in the necessity for monitoring. In this first quote, a CEO refers to the difficulties one of his colleagues encountered with users who wrote hate speech and used the organization's computers to broadcast it anonymously over the Internet:

I: Has [hate speech] happened here?

R: Not here, but it's happened in other places and I have seen that… Every society has idiots and bigots and so on. There is a small percentage, but the Internet gives them access to an audience where they don't have to accept responsibility for it.

This idea of the "small percentage" of individuals who abuse their privileges came up frequently as a managerial justification for conducting monitoring of IT and resources. Managers generally espoused the rationale that the majority of employees were honest and hardworking, but that the inevitable presence of one bad apple made it necessary to use monitoring

techniques to track the computer activities of all employees. When we dug for details, however, we frequently found that the available data contradicted the cheery one bad apple story:

I: We talked in our last interview about the ability of the system to monitor the activities of employees. I was wondering how confident you feel about the [new] system being able to handle the security.

R: It's very good. Because we do that, (sigh). Where I was employed before, they had [the same software]. When you go to log onto the terminal, if it takes more than three times, it locks the terminal, if you don't get the right password, and it generates a report. Someone screens those reports. We found out that people were doing that to find out passwords, because they were locking them up all the time… I mean, I don't want to be big brother on them, but there's benefit to it.

Other respondents in this same organization told us, for example, that some employees were using the system to try to look up the medical records of individuals for whom they were not involved in care. This behavior became widespread when a local celebrity arrived for treatment. Although it may be true that the majority of employees are honest and scrupulous, we found that data collected from monitoring and surveillance systems sometimes contradicted the "one bad apple" theory offered by managers. Curiosity and other benign motivations may prompt a proportion of employees to extend the boundaries of acceptable use further than managers may have believed likely. The following respondent expresses the belief that a signature on an employee confidentiality agreement is not sufficient to ensure such compliance and that a monitoring function is needed to "track" the compliance of employees' actual behaviors:

I: Are there policies related to [confidentiality]?

R: Yes, we have written policies, and there's confidentiality, and we have compliance, that's the buzz word now, corporate compliance, so they yearly have to sign this thing about confidentiality and corporate compliance, and everything else. Words on paper, you know… Just signing a statement isn't a big thing.

Despite the above respondent's cynicism about the value of signed statements, we found it common for organizations to require employees to sign such agreements. Sometimes, one component of such statements is an explicit notice to employees that such monitoring is a condition of employment. One final justification offered by managers for conducting monitoring and surveillance was based on the legally correct argument that the organization owned the equipment that the employees were using to do their jobs, and so the organization had both a right and an interest in policing the use of those facilities:

I: How will you handle monitoring of emails?

R: [We can] develop some policies and standards of practice on how you use it, what's acceptable and what's not. People would have the understanding that it's our right, it's our property, and it's our email. It's on our system. We technically have the right to go in and look at it any time we wanted. As long as they understand that (laughs). And we do have two unions, so this becomes an issue.

I: Have you done any communication with the unions about this?

R: We haven't done any formal communication with the union representatives.

Unions have generally been advocates of limitations and restrictions on the use of monitoring and surveillance in organizations and frequently take the position that these practices constitute both an invasion of worker privacy and a goad towards unreasonable productivity standards (Bain & Taylor, 2000; Westin, 1992). Managers with whom we spoke typically reported awareness of this position held by unions, but also cited the justifications noted above as trumping union concerns.

To summarize, managers noted examples of problematic user behavior that illustrated the organization's interest in monitoring user behaviors. Managers offered regulatory compliance as a driver for the use of monitoring, and justified confidentiality agreements to employees–including clauses accepting the organization's monitoring practices–on the basis of such compliance. When pressed on the rights issues involved in monitoring and surveillance, managers cited ownership of the computer and equipment networks as a rationale for giving unfettered access to records tracing employees' computer-related behavior.

Perspectives of Information Technologists

Turning now to IT professionals, we present verbatims concerning monitoring from six interviews. In many instances, IT people set up monitoring in such a way as to provide reports and information to non-IT managers (e.g., in human resources), but even in these cases the IT people typically have substantial access to the monitoring data. Sometimes this monitoring was primarily used for technical reasons – such as avoiding viruses – as the following exchange shows:

I: Is there an information security policy that you know about?

R: Our tech support takes care of that. And they have pretty much set their guidelines and pretty much stick to them.

I: Do they monitor what other employees do?

R: Yes they can monitor… they usually monitor right from the server. Mainly it is email and Internet that can be monitored. Email they have to because it just comes in and grows, and that is where you get lot of your viruses come through and so we have to make sure it doesn't get past that server and they are really good about that.

Monitoring network traffic, even for technical reasons such as virus mitigation, gives IT staff access to records of employees' activities. This high level of access can generate ethical quandaries by putting the IT professionals in possession of sensitive information about employees' behavior. We found that many of our respondents were uncomfortable with this degree of access, to the point where they ignored or softened policies set by higher management:

I: Do people ever wonder how much access you have to their information, to their emails?

R: No I make sure everybody knows that [we] have access to everything… I assure them whenever of my personal ethics on confidentiality and all that stuff, I never let them become compromised. So I haven't had any issues with people caring about how much access I have. But, I'll share an incident with you that was a little troubling to me. I worked for a company where there was a disgruntled employee and there was a lawsuit involved. I got a call from person above me that they wanted me to capture all of this person's email and make it available to them. I know legally that all mail in an electronic system owned by a corporation, business, is a property of that business. But I thought I felt badly about walking a fine ethical line. I felt I would compromise that employee. It was troublesome to me.

The following respondent contrasts the harshness of the stated policies about monitoring and actual practices:

I: Will there be any other information in the system about employees' computer use or activities?

R: We are just writing the policy and we just wrote up this policy statement which basically says that we are policing everything they say and do all day long. It's not really true. Yes, we do have the tools to monitor, but no, we don't really want to do that. They are pretty conservative here about the policies, but we would rather give people the benefit of the doubt, that they are using the tools given to them in the best interest of the organization.

We found that harsh policies and gentle practices were a common combination. The tendency for harsh policies probably reflected managers' desires to protect the organization against the rare instance when an employee does commit an offense. The same respondent made a distinction between the rare case with significant impact and the more typical problem that may cause annoyance but is otherwise harmless. The respondent seemed to see value in monitoring of both serious and merely annoying behaviors, although the comments made clear a preference to leave policy-abiding employees alone. The following comments suggested a certain intentional laxity in enforcing monitoring policies:

I: Do they monitor all [employees'] email?

R1: Well, they don't monitor… No, no, they don't monitor per individual per se. In other words they won't go into your email and see what is in there. That they don't do, but they monitor as it comes in to see what IP address this is going to and they don't necessarily know who that belongs to but they can see what is coming in. If there are a lot of viruses coming in then they are getting a lot of hits but actually monitoring and checking people's personal email no.

R2: I don't want to monitor or even have people think we are. I would like to make these tools encourage the most efficient forms of communication: quick, fast, and okay as long as it goes by certain guidelines… We don't want litigation… I am hoping that it will make people comfortable that we have a policy, people know what it is, and if anyone asks anything, we can show them the policy. Hopefully they won't necessarily look for a minute-by-minute policing of what the policy says.

While managers hand down policy statements that mandate extensive, continuous monitoring of employee behavior, some IT professionals appear to have a desire maintain their faith in the basic goodness of people and with that desire a preference to avoid prying into people's behavior. As a result, some IT people intentionally avoid using the monitoring tools available to them or to use them in a limited way:

I: How comfortable do you feel with setting the security priorities?

R: I feel comfortable, again, as long as I am involved in what the technology can do for it… But I also have a social conscience. Privacy needs to be maintained, and our customers deserve that. But I recognize the challenge where they need expedited [service] and the people need information right away, so somehow you have to rectify that discrepancy. If I allow a weakness in security policy, and gain something in [service], from a social conscience perspective, I have made the right decision.

This respondent's "social conscience" constrained him from implementing the strictest possible security policy. This idea seemed to signify a balancing act among the needs of different groups–privacy of customers, security of the organization, organizational efficiency/productivity, and rights of the employees–that this IT professional felt responsible for performing. Thus some IT people seem to recognize that security and efficiency are not "universal goods" to be achieved at the expense of other desirable outcomes.

Employee Beliefs about Monitoring

When examining how employees felt about electronic monitoring and surveillance (five interviews excerpted here), we found that there were two essential perspectives reported. One group was skeptical of monitoring. The other group expressed trust in their management's ability to responsibly collect and protect sensitive data. Many in this camp seemed to have little awareness of the monitoring technologies in use, the frequency with which they were monitored, who had access to the data, and so forth, even in firms with written policies that employees were obliged to sign:

I: Do you know if your work is monitored regarding this?

R1: I would think it is. I don't pay very much mind because other than an occasional email to an individual in the family every three days or something like that, I don't misuse it, so I don't worry about it.

R2: I don't think there are any restrictions. We sign something when we first start working when we do our paperwork and I think that says no personal use, but I don't think there's any type of restrictions, I don't know whether there's monitoring or not.

We found this to be a very common attitude: "Because I personally am honest, I do not worry about how my behavior is being tracked." This situation is emphasized below by a customer service agent who whose initial response of laughter about the question itself reveals as much about the organization and its informal culture as the rest of her explanation:

I: Do you know if your work is monitored?

R: (laughter) I don't really think so, because I don't think that anybody in [our company] as far as I know misuses the Internet… And we do have a trust basis. If we saw somebody that was always on the Internet and they were out shopping or something like that we would address it. If it became a problem, we would, but we don't really look over anyone's shoulder.

We found that this phrase, "trust basis," was a common expression among managers, employees, and IT professionals alike – particularly in smaller organizations. The phrase seemed to indicate something of the family-like nature of the smaller firms. The relationships among the members of the organization helped to ensure that everyone kept his or her behavior within the expected norms. Along the same line, many users thought that the administration had a right to monitor them as long as they were told about the procedure and consequences ahead of time.

In contrast to the smaller settings, larger institutions included more employees who were skeptical at the prospect of their employer using or increasing monitoring activities. Some employees viewed monitoring as an implication by management that they – the employees – were not trusted. Others thought that monitoring did not accurately reflect their workplace activities. Anger and fear were expressed by some employees at the idea that monitoring would not be used sensitively. The individual quoted below imparted his thoughts about the possibility of a centralized computer system with increased monitoring capabilities:

I: Do you have any other questions?

R: I have had the problem in the past the people try to quantify things too much. They make a justification for wanting to monitor us, and that's not really a problem in itself, because I know we work hard here. It's just that (pause), well, the numbers don't always reflect the reality… My fear is that there would be repercussions for me if it looks worse on paper than it really is.

This employee was one of many with this type of concern. These two employees' irritation is displayed in their comments about the prospects of increased accountability for workers' time:

I: Why is management interested in [implementing a new system in which clients verify provision of service?]

R: They think that we [employees] are wasting time, and that they [management] have no accounting for our time; that they will have closer tabs on us. But you hear in the back of the office sometimes, "I don't want to be treated like a baby. I don't want a babysitter. I am here to do my job and however long it takes, it takes."

To summarize, in smaller organizations there was little concern and little awareness of what kinds of monitoring were being conducted, even in companies that were in fact using multiple monitoring techniques. In these organizations, employees reported sentiments about their own innocence and the degree of trust that they felt in the organization's capability for treating them fairly with respect to monitoring. In larger organizations, employees expressed reservations about monitoring, generally on one of two bases. First, some employees felt that making employee data more visible also implied a loss of autonomy. In effect, the sentiment was that if managers can see what I'm doing, they will want to control it, to the detriment of my freedom. The other basis for employee concerns about monitoring pertained to the inability of monitoring to give a clear picture of what employees were actually doing. Here, employees felt that their honest, productive activities might sometimes be erroneously detected as inappropriate or contrary to organizational policies.

INTERPRETATION AND ANALYSIS

If monitoring is a key part of holding employees accountable for their security-related behavior – and it is certainly a key ingredient in enforcing security policies – the question arises of how monitoring can be conducted in a fair, acceptable, and effective fashion. Managers and IT professionals expressed similar sentiments regarding the necessity for monitoring employees' computer and network activities. IT professionals discussed the necessity of monitoring based on their knowledge of problems that arise on the organization's information systems. Simultaneously, however, some IT professionals expressed squeamishness about their responsibilities with respect to monitoring. The closeness of the IT people to the details of monitoring processes ensures that they will encounter records of employee behaviors – good, bad, and everywhere in between – and some of our respondents felt uncomfortable about this.

Perhaps for this reason, IT professionals carefully explain their own ethicality and the controls they used to avoid misuse of monitoring data. In addition, we saw examples of intentional laxity in the enforcement of monitoring. When IT people found the organization's policies too harsh, they tended to soften monitoring practices to mollify their own concerns for fairness. In earlier examinations of IT professionals, researchers found that these people felt caught in a dilemma: Management demands for policy enforcement exerted pressure in one direction, while social ties and concerns for the well-being of employees (and IT people's own reputations) exerted pressure in the other direction (Stanton & Stam, 2003). Although some might say that IT people get paid to resolve such conflicts, it seems risky to have an intentional gap between stated policy and actual procedure that must always be closed by judgment calls.

In contrast, managers seemed insulated from the messy reality of monitoring. When asked about the rightness of monitoring, almost all managers reported the justification that the organization owned the equipment and therefore had rights to maintain records of all activities involving that equipment. This perspective is correct, in a purely legal sense, but seems unsubtle. The tone of these conversations always created the sense that managers were following the "party line," and that they were reluctant to say what they really thought about justifications for monitoring (or perhaps, lamentably, they had just not given the matter much thought, particularly with respect to the technical benefits related to security). Although IT people recognized the ownership rationale, they were generally quick to temper the blanket statement of ownership with qualifications about fair and reasonable treatment of employees. For their part, employees rarely mentioned an awareness of the ownership rationale.

In fact, employees in organizations we visited seemed unconcerned about monitoring. A common belief was that monitoring was customary; therefore the respondents had no major concerns about it. A few subtleties lingered under this calm surface, however. First, some employees mentioned quiet plans of how to escape from monitoring, starting with the relatively benign step of using a free email account for personal correspondence. Likewise, we heard reports of the "nothing to hide" rationale: Employees indicated that they had no concerns about monitoring because they themselves were innocent of wrongdoing. In many organizations, employees' evaluations of their organizations' practices as typical made it unlikely for them to ruminate deeply about the fairness implications of those practices. The exceptions arose in situations where trust in the organization had been eroded by previous technology adoption failures, or where the proposed changes to monitoring practices looked to the employees like an attempt on the part of management to exert more control over them.

Monitoring becomes a threat to employees when workers see it as controlling or unfair, when trust has eroded between employees and managers, and/or when abrupt changes to monitoring-related policies occur. To obtain the security benefits of monitoring it is necessary to engage employees in this aspect of security governance. Our recommendations for security governance focus on improving communication between managers, technologists, and employees about monitoring; using a consultative process to develop policies, monitoring practices, and enforcement strategies; and using a public, community-based approach for enforcement. We argue that a critical aspect of transparency in information security governance is making the methods of monitoring visible, public, and widely understood in the user community. Making monitoring transparent occurs in three ways: publicizing techniques, publicizing results, and publicizing enforcement outcomes. By working to

establish an environment in which accountability and integrity can thrive, organizations can ensure that those individuals who handle and process the organization's data have the support they need to reduce security risks. Our research suggests that organizations can take steps toward this ideal through developing the processes of transparent security governance.

REFERENCES

1. Bain, P., & Taylor, P. (2000). Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment, 15* (1), 2-18.
2. Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns, Computer & Security, 20 (2), 165-172.
3. Stanton, J. M. & Stam, K. R. (2006, Forthcoming). *The Visible Employee*. Medford, NJ: Information Today.
4. Stanton, J. M., & Stam, K. R. (2003). IT, Privacy, and Power within Organizations: A View from Boundary Theory and Social Exchange Perspectives. *Surveillance and Society, 2*, 152-190.
5. Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. Human Performance, 13, 85-113.
6. Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn, Socio-Technical and Human Cognition Elements of Information Systems (pp. 79-103). London: Idea Group.
7. Straub, D. and W. Nance (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly, March 1990, 45-60.
8. Westin, A.F. (1992). Two key factors that belong in a macroergonomic analysis of electronic monitoring: Employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics, 23*, 35-42.Ajzen, I. (1988) Attitudes, personality, and behavior, The Dorsey Press, Chicago.