

**Ethical Considerations for
IT and Security Professionals**

Perry Carpenter, CISSP, CIPP

January 6, 2007

Introduction

Information Security and Information Technology professionals wield much power as part of their daily jobs; and, as the saying goes, “with great power comes great responsibility.”¹ This paper will examine how that power should be used ethically and responsibly. Specific consideration will be given to topics related to employee monitoring, separation of duties, and access controls.

General Considerations

Information Security and IT employees generally require at least *some* elevated privilege in order to perform their jobs. Just privileges include the ability to create, modify, or delete accounts; the ability to assign users to access groups; or the ability to view sensitive data elements (such as a user’s Social Security Number, access logs, etc...). Further, regulations at the state or Federal level may require that companies employ more granular monitoring of user activities.

Increasingly, vendor solutions are becoming available which will allow companies to employ monitoring strategies more easily than ever before. Such technologies range from many of the “content filtering” solutions (such as are available through companies like Vontu, Vericept, Tablus, and Oakley Networks) to advanced auditing solutions (such as those available through NetIQ, IBM Tivoli, SenSage, and others). As these technologies become more powerful and agile, so does the necessity to ensure that they are implemented responsibly and ethically.

In addition, and due to the myriad of reported data breaches² coupled with dramatic media exposure³ and the continuous onslaught of miscreants seeking to defraud the public of their personal information; for example, the public is now *very* aware of concepts such as phishing⁴ and that there are groups seeking to trick them into giving up the very information necessary to establish an identity or to commit financial fraud.

With the current level of public awareness of issues related to privacy, it is incumbent upon companies to ensure that proper policies and procedures are established and followed. IT and Information Security staff members, specifically, should receive information and training related to the importance of following proper procedure. Additionally, such training should not be limited to IT and InfoSec staff members – targeted training campaigns should be developed for upper management, the marketing department, call center employees, etc... In other words, it is everyone’s responsibility to act ethically and to protect the data with which they have been entrusted.

¹ As far as I can tell, this saying was popularized by Stan Lee’s use in the Spiderman mythology. However, I doubt that he was the originator of the phrase.

² See the Privacy Rights Clearinghouse Chronology of Data Breaches for more info.
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

³ A good example is CNBC’s documentary, “Big Brother Big Business.” See:
<http://www.cnbcbigbrother.com/>.

⁴ As demonstrated by the fact that the current “leading” web-browser, IE7, comes standard with an anti-phishing toolbar.

Employee Monitoring

There is no doubt about it-- America and Europe are becoming societies in which the populous is almost continually monitored. CCTV cameras, both conspicuous and inconspicuous, are interspersed throughout most public areas such that the majority of a person's "public" activities are monitored. Further, most companies have similarly employed CCTV systems to monitor the activities of employees, visitors, vendors, and contractors.

In most instances, the individuals being monitored are aware that such activity is occurring. However, in order to monitor ethically, companies should require that the employees receive clear notice that their activities are being monitored. The notice should be easily understood and should explicitly outline the types of monitoring which will occur. The author's recommendation is to create a policy which outlining the type of CCTV monitoring occurs, what type of network activity is monitored, if telephone monitoring occurs, and so on. In many cases, a company may wish to use these examples and state that employees, while on company premises, should have no expectation of privacy whatsoever. Lastly, employees should be required to sign a form which states that they have read and understand the policy.

The implementation of monitoring systems and the establishment of a monitoring policy comes the need to define processes, procedures, and policies related to employee investigations. The company needs to clearly define steps related to what parties can review the monitoring data and how access of the data will be audited. These questions, while posed in the context of employee monitoring, are broader – and will be considered in the next sections.

Separation of Duties and Access Control

A key concept of security is "separation of duties." A properly implemented separation of duties strategy will ensure that, in order to perform a malicious or nefarious act, collusion is needed. For example, separation of duties should ensure that an employee cannot fill out a timesheet, approve the timesheet, submit the timesheet to payroll, print the paycheck, and sign the paycheck. In this example, it is clear that, in order to keep people honest, separation is needed.

Similarly, such separation should be established in areas such as user account creation/maintenance; the establishment, approval, and application of security roles; and the requisition, viewing, management, archival, and disposal of log data, audit trails, and monitoring data. If proper separation is not employed, there is a chance that those tasked with managing the data will become voyeurs, or will find ways to use such data for personal advantage.⁵ Thus, network monitoring alarms, employee investigation requests, and so on, should be routed such that a single person cannot circumvent the intent of such systems.

⁵ Wilson, Tim. Security's Rotten Apples. *Dark Reading*. October 4, 2006. http://www.darkreading.com/document.asp?doc_id=105282.

Just “doing the right thing”

In many instances, the best way for a company to determine the ethicality of a practice is to perform the “smell” test. In other words, when the practice is explained, does it stand up as having integrity – or is something clearly or intuitively “off?” Companies should understand that this is how employees, the media, stakeholders, and lawyers are likely to evaluate their practices. In the eyes of the public, just because a practice is “legal” does not mean that it is acceptable.

A good example of this is the treatment of customer data by 3rd party data brokers, marketing firms, and the government. Most consumers are shocked when they realize the breadth of data that companies have about them and their personal habits. Upon learning of the vast amounts of data collected and aggregated, they are usually further troubled by the fact that the amassed data is sold for marketing purposes by companies such as Acxiom, Experian, and others. One has to wonder, before this industry was allowed to be created, if a “smell” test was performed...

Conclusion

Companies require a practical method for ensuring that employees act ethically and that company policies and practices are developed in such a way as to require ethical behavior. Ensuring separation of duties, being forthright regarding practices related to monitoring, and by employing the “smell” test, companies will be on their way to establishing credible, respectable, and ethical practices.