Employee Monitoring

Whether and How to Implement an Employee Activity Logging Program

In deciding whether, how much, and how to monitor employees' use of IT resources, organizations must wrestle with the balance between protecting corporate interests and respecting employee privacy — and there is no one-size-fits-all answer. A company that fails to plan, communicate, and execute a logging strategy properly can do serious damage to employee morale, while still doing little to reduce the risky behavior the strategy is meant to fight. This paper outlines the pros and cons of tracking employee activity and presents a methodology for creating a logging strategy that avoids potential pitfalls.

XANTRION
CYBERSECURITY • IT SUPPORT

You may know why you want to monitor employee activities, but your employees need to know it, too—and they need to understand that they, too, have something to gain.

Potential Benefits and Drawbacks

The arguments in favor of monitoring employee activity are many and varied. Logging can help organizations spot and mitigate the misuse of corporate resources. It can ensure compliance with human resources policies and government regulations that protect sensitive and confidential data, while providing an audit trail in case the organization is challenged. Logging can protect against insider theft or abuse of intellectual property and mitigate the risk of a violation. It can even help managers pinpoint underperformers and identify ways of improving their performance, as well as spotlighting top performers and capturing their best practices for sharing.

However, businesses cannot ignore the potential downside of logging. Employees may perceive it as an invasion of privacy or an insulting suggestion that they can't be trusted. Worse yet, a logging program might accidentally capture an employee's personal data, like a banking password or confidential health information, putting both the individual and the company at risk if that protected data is exposed to misuse or abuse.

An organization that wants to ensure employees are using IT resources appropriately needs to balance these conflicting challenges in determining whether to log activity at all, which types of activity to log, and how to do so both effectively and unobtrusively.

Ensuring a Successful Logging Program

Clearly Define and Articulate Your Goals

You may know why you want to monitor employee activities, but your employees need to know it, too—and they need to understand that they, too, have something to gain. Writing out the benefits of a properly implemented and managed program will clarify your goals for everyone affected. These are some of the issues you may want to address:

- Maintenance of a productive, professional environment. Everyone wants this, but few people are willing to step up to report problems. All employees look to management to ensure that their co-workers are hardworking and that the workplace is free from harassment. Activity logging lets management investigate concerns based on observable, reported facts. This protects people from unjust accusations while providing a concrete basis for behavioral counseling if warranted.
- Protection of intellectual property. All firms are vulnerable to some extent to harm resulting from compromise of their intellectual property, from trade secrets to client lists. Any impact on the firm will necessarily reverberate to employees in the form of layoffs or reductions in compensation. Employees and employers alike share an interest in preventing firm information from being leaked for personal gain.
- Protection of client confidentiality. Privacy protections aren't just common sense; they're the law. Regulations including the California Privacy Act, HIPAA, and SEC regulation S-P, to name just a few, mandate measures to protect private client information. Logging can be an effective tool to ensure compliance with a firm's privacy policy and to prove compliance in case of an audit.
- Protection of company finance. Logging allows companies to investigate suspicious activity to determine whether or not it indicates an actual problem — a particular benefit given how often internal fraud goes undetected for long periods of time. Criminal organizations will often compromise the workstations of people with authority to transfer funds in order to commit funds transfer fraud. Detailed review of the activities on these workstations can help detect fraud as it happens or provide forensic evidence after the fact.

Involve All Stakeholders in the Planning Process

As with any organizational change, establishing a logging program requires the inclusion of every affected constituency:

- Executive management
- Human resources
- Legal
- Information technology

- The general employee population, focusing on those who are
  - Influential
  - Important to the organization—whose concerns are worth trying to work through
  - Likely to have concerns—if you can solve their concerns then you have likely covered the concerns of the average employee

Ensure Awareness of Firm Policies and Consider How Logging is Disclosed

While most logging programs start with the intention of rooting out malicious activity, they often do more to uncover accidental violations. It makes no sense to monitor noncompliance with corporate Acceptable Use policies if your employees are unclear on what those policies are and what compliance looks like. Even if they have read and signed off on them, they may not fully understand the provisions. Because the vast majority of Acceptable Use violations are likely to be inadvertent, logging can be a powerful tool for auditing employee training and finding areas where it can be improved. First, though, you must clarify what the Acceptable Use policies are, as well as the penalties for violating them.

At the same time, it may not be necessary or even desirable to disclose exactly what types of activity you monitor or how you do so. Greater transparency builds trust within the organization, but it also tells bad actors precisely how to subvert the safeguards you set up.

Determine What to Log

Determining what to log will vary based on each organization's specific needs. Expect to face difficult decisions about what to include, what to exclude, and which uses you consider legitimate or harmful. These areas require particular attention:

- Social media (Facebook, Twitter, etc.). You definitely want to know whether an employee is posting inappropriate material using company time or resources or spending excessive time on non-work activities. You may or may not want to prohibit occasional access. However, you do not want to capture employees' personal information.
- Financial websites . You want to detect potentially fraudulent activity. You do not want to capture employees' personal passwords or financial data.
- Email and filesharing services (Dropbox, Box, etc.). These are prime mechanisms for inappropriate dissemination of corporate information, so you will need to determine how much oversight you need. Most of the time, though, your employees will use them for legitimate communications that you have no need to restrict.

In general, assume that your choice is to trade off specificity for trust: if you monitor all employees at all times, for example, you avoid any perception that you're unfairly targeting specific individuals, but it will raise employees' overall concerns about privacy.

Controlling Access to Logged Information

Your company must maintain a balance between its right to know how employees are using resources and employees' rights to and expectations of privacy. Once you determine what to log, the next step is determining who can see the logged information and under what circumstances. These questions will help you clarify your strategy:

- Do regulations or other requirements call for regular activity audits whether or not the company has spotted specific activities?
- Should you restrict access to logged activity by requiring at least two people's credentials for review? What other administrative controls should you put in place to control who can access activity logs?
- Do you need to set up automated alerts that trigger a review of logs — for example, when your systems detect credit card numbers, Social Security numbers, or certain phrases in email?
- How long should data be retained? A shorter period tends to be more respectful of employee privacy, but annual audits may require longer periods of data retention.

Your company must maintain a balance between its right to know how employees are using resources and employees' rights to and expectations of privacy.

Technology and Cost Concerns

Currently, the direct cost of a logging solution is relatively low: software that costs roughly $30 per employee per year, plus minor storage and compute costs. Modern network management makes it simple to install logging agents on every computer enterprise-wide, and most logging software is invisible to the end user.

Our Experience

Implementation and maintenance of activity logging is both simple and inexpensive from a technological, and budgetary point of view. However, the legal, HR, and morale ramifications can be significant. Therefore, Xantrion urges companies considering monitoring employee activity to plan carefully and communicate clearly with employees at every step.

Xantrion provides the expertise and the skilled people necessary to assist you with cybersecurity issues. We can help with everything from topics such as employee monitoring to consulting with you on appropriate approaches to other security challenges. Since we have successfully implemented best practices for ourselves and for multiple clients, we know the pros and cons of various approaches as well as the implementation pitfalls.

Give us a call at (510) 272-4701 or visit https://www.xantrion.com/it-roadmap.html and let us know how we can help.

Ready to learn more?
Get the latest news and IT tips from Xantrion.

Subscribe

XANTRION
CYBERSECURITY • IT SUPPORT

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

(510) 272-4701