White Paper

Advantages of Company-wide Monitoring over
Focused Employee Investigations

Table of Contents

Introduction

If a company is considering the purchase of software to conduct a focused investigation of an employee suspected of unethical or illegal activity using company PCs and the Internet, it will benefit by first reviewing the advantages of centrally managed, company-wide monitoring. This monitoring philosophy is becoming the norm for many companies of all sizes worldwide because properly implemented, such a plan increases productivity, minimizes liability, plus the industry's leading software is remarkably powerful, surprisingly affordable, and easy to install, deploy, and maintain.

In addition to permitting the efficient activity monitoring of all company employees over time, an effective centrally managed, company-wide monitoring solution will also provide companies with the ability to specifically focus on one or more employees or departments. Using this "Big Picture View" approach with easy to customize graphic charts, companies will not only detect narrow instances of abuse, but will increase productivity by monitoring broader trends and patterns of how employees are using company PCs and the Internet.

Background

When an employee is suspected of unethical or illegal activity, management usually conducts an investigation focusing exclusively on the individual. This approach is effective for confirming suspicions and for documenting infractions, but management needs to question if these problems exist elsewhere within the organization. Neglecting abuse can only serve to increase liability by putting a company at risk.

For example, banks generally install surveillance cameras at all their locations, not just at the branches they feel are highest risk. The primary reason for doing so is to deter crime based on the presence of the cameras. However, from a purely functional perspective, the cameras are installed to record information for the authorities to examine if a crime is committed. If a bank neglected to install surveillance cameras at any one of its branches, in time a thief would recognize the weakness and exploit the vulnerability of that branch.

The same mindset applies to employee monitoring. Unethical activity often occurs where it is least expected. The company-wide monitoring approach serves as a deterrent to unethical or inappropriate behavior. In addition, company-wide employee monitoring significantly boosts employee productivity.

Increasing Productivity

It has been shown that if an employee knows they are the subject of ongoing employee monitoring, they are likely to stay on task. For example, if an employer can detect when an employee starts and stops working, the employee will have a tendency to work longer hours. If the employee knows the employer has an ability to detect weak work habits --such as long or frequent breaks and extra-long lunches on a regular basis -- the tendency will be to minimize them.   If the employee knows the employer can detect visits to nonwork-related websites or online searches for items having nothing to do with work, then the abuse will be less likely to occur.

Employees may not be doing anything unethical or illegal but productivity still can be impacted heavily by individuals using company PCs and the Internet for personal use. It has become an industry "rule of thumb" that every employee spends at least one hour each day doing exactly that. Detecting this behavior and taking corrective measures to minimize or eliminate it will result in increased productivity.

Reduce Liability

Companies can put themselves at risk by conducting a focused investigation of an employee, especially if it results in termination of employment. To eliminate the potential of a lawsuit based on discrimination, it is wise to adopt a company-wide policy to unconditionally monitor all employees. This action will ensure a discrimination claim never sees the light of day.

Detection of Unethical or Illegal Activities

Employees often make copies of customer lists and other company-owned information. They usually print these files out, or copy them to USB sticks, or transfer them to remote sites, or they simply send an email with attachments to a personal email account.   Sometimes this is done legitimately, but if and when it is not, will you be in a position to detect it? Company-wide monitoring empowers the detection of all these scenarios by revealing abnormal and suspicious patterns.

For example, every day thousands of employees resign and announce plans to work elsewhere. If the employee is retained through the traditional notice period, they are usually placed under watch ... but often it is too late because acts of digital theft typically occur prior to resignation. If employee monitoring software is installed on only a handful of computers, an employer finds itself in a hit-or-miss situation when it comes to uncovering and documenting illegal activities. With company-wide monitoring, management can see if digital theft occurred in the weeks leading up to the resignation, even if the activity occurred on multiple PCs. Obviously, this is impossible with a product installed only after the employee has committed a suspicious act.

About Spector 360®

Spector 360 enables you to monitor employee PC and Internet use, analyze trends and patterns, search for specific details, investigate when something seems amiss, and report your findings all from the convenience of your desktop. Spector 360 is a highly scalable, centrally-managed, employee monitoring solution that is easy to deploy and manage, even company-wide.

Features at a Glance

- Monitor all employee PC and Internet activity with high-level charts, graphs and tables
- View detailed activity of individual employees with point-and-click drill down
- Automated reporting
- Includes context-based web filtering
- Multiple levels of security prevent tampering or disabling
- Configure, install and manage over existing network

"Top-notch reporting and monitoring"

"Highly configurable and scalable"

"Well-designed client server architecture"

September 2008
Spector 360   **-PC Magazine**

Consider another scenario, one in which employees use Chat or IM to communicate. Anecdotal evidence suggests this has become the medium of choice for flirting between co-workers, an activity ripe for inducing a sexual harassment claim. Using company-wide monitoring, if and when such a claim is made, Human Resources and/or other management will be able to use recorded Chat or IM sessions to evaluate the evidence.

Further, if an employee is conducting online searches using terms such as "drugs", "sex", or "guns", management needs to know. Using popular features available on effective company-wide monitoring software, management will be able to determine the employees generating the most keyword alerts, especially when the used terms have illicit or unethical connotations.

Conclusion

Spector 360 Employee Monitoring Software satisfies all of industry's PC and Internet Activity monitoring requirements — and more — empowering companies to keep a pulse on business while increasing workforce productivity to unprecedented levels. Using Spector 360 to adopt a company-wide approach to employee monitoring will reduce liability, help achieve investigative goals, and empower you to react to virtually any situation concerning your employees and how they use company PCs and the Internet.

◇◇

SpectorSoft offers PC and Internet monitoring and surveillance solutions for education, business, government and home users.

To learn more, and see how Spector 360 monitoring software can help solve your workplace Internet abuse and productivity issues, please visit **spector360.com**.

Learn more about SpectorSoft monitoring and surveillance solutions for business at **spectorsoft.com**

SpectorSoft Corporation
1555 Indian River Blvd.
Vero Beach, FL 32960

888.598.2788 toll-free
772.770.5670 sales and support

www.spectorsoft.com