Implementing an Employee Monitoring Program

SpectorSoft

Introduction

Monitoring employee computer activity has significant benefits:

• Increased security against insider threats

• Reduced risk via:

    o Early detection of fraudulent activities

    o Detection of potential HR issues that might otherwise only come to light in the form of a complaint or litigation

• Improved operational efficiency achieved through:

    o Baselining activity of top performing employees and departments to establish best practices and improve training programs

    o Tracking adoption of new policies and applications enterprise-wide, helping to insure ROI goals are met and investments fully utilized

• Productivity increases driven by:

    o Identifying employees having trouble staying on task so that they can be managed effectively

    o Identifying the top "time drain" activities enterprise-wide; implementing and tracking adherence to policies designed to maximize productivity

• More efficient and effective employee investigations, leading to:

    o Termination protection – documentation of justification to head off wrongful termination claims

    o Reduced cost associated with investigations

    o Reduced time spent assembling evidence in an investigation

    o Elimination or reduction of reliance on expensive, specialized skill sets required to conduct forensic investigations

Security & Risk professionals recognize the value and benefits of implementing an employee-monitoring program. Privacy advocates and Legal and Human Resources professionals see potentially unwarranted invasion of employee privacy as reasons not to monitor, or at least to restrict monitoring to instances where enough "probable cause" exists to warrant tilting the balance between the privacy of an employee and the interests of the company.

This document is intended to assist company executives determining whether or not to implement employee activity monitoring.

Decision Point: Why Monitor Employee Activity?

The decision to begin recording employee digital activity is usually made for one of two reasons:
• **Reactive Investigation:** Something bad has happened or there is suspicion that something bad has happened or is about to happen. The organization has cause to investigate a person or group of people.
• **Proactive Protection Strategy:** The organization seeks to improve its internal security against insider threats, insure adherence to company policies, and improve awareness about what is happening within the company.

The Reactive Decision

When an investigation is required, the decision to implement an employee monitoring solution is easy. Something triggered the need to look more closely at employee activity. While there is no cookie-cutter approach to employee investigations, Management, HR, and Legal are generally heavily involved and upfront in the decision.

The organization has already determined that the balance between the needs of the organization and the privacy of the employee must tilt to the organization.

The Proactive Decision

The decision to implement proactive employee recording is more difficult than kicking off an employee investigation. The proactive approach requires logging digital activity of employees in the absence of a trigger. In addition, for maximum effectiveness, proactive monitoring must be widely deployed.

Without a trigger and probable cause (any known reason to take a closer look), the organization is less comfortable tilting the balance towards the needs of the company. The privacy of the employee is of greater concern.

Decision Point: What is Right for Your Organization?

Is there a way to implement employee activity monitoring that aligns to your corporate culture and values, the legal considerations where you do business, and the needs and goals that have you considering employee monitoring?

Where to Start

While every organization is unique, there are some broad guidelines that can help you make the best decision for your company.
1.   Determine your goals - review your Acceptable Use Policy
2.   Consider involving your employees
3.   Decide whether to implement active, passive, or both types of monitoring
4.   Decide what to monitor and what data to retain
5.   Decide how to handle escalation and review

SpectorSoft

Get the Stakeholders Together

Company size and structure will determine who needs to be in the room. As a general rule, include the most senior person in the organization, as is possible, in these decisions.

• **Senior Management:** The CEO or someone designated in his/her stead.

• **Human Resources:** The head of HR as someone who balances the needs of the company and of the employees every day.

• **Legal:** Your General Counsel or whomever you go to for advice on legal matters.

• **Information Technology:** An IT expert who will be involved both in evaluating possible solutions and implementing the solution you select.

Decision Point: What are Your Goals?

Detect Insider Threats

If you are concerned about insider threats, it's important to talk through the challenges of detecting and deterring them. Non-technical stakeholders may not know coming in that traditional security solutions are (a) largely focused on perimeter security and (b) not intended to identify or prevent problems stemming from insiders who have been granted authorization to access sensitive data or systems.

So, for example, data theft by an insider may go undetected for a long period, or, in the worst case, until you read about it in the news. Employee fraud may go unnoticed until the annual audit, if it is noticed at all.

Inadvertent vs. Malicious Breaches

Expect a discussion on monitoring activity to touch on the fact that it's likely only a small number of employees might be engaged in behaviors that are problematic. Be prepared to talk about the difference between inadvertent breaches or policy violations and intentional, malicious ones. Focus on the resultant damage, not the intent.

Resources for Discussion

There are some great resources available to help frame the discussion and help you establish the right goals for your organization.

The Association of Certified Fraud Examiners ("ACFE") Report to the Nations on Occupational Fraud and Abuse is a fantastic source of information on the various types of fraud being committed, and the damage that fraud causes to a companies bottom line.
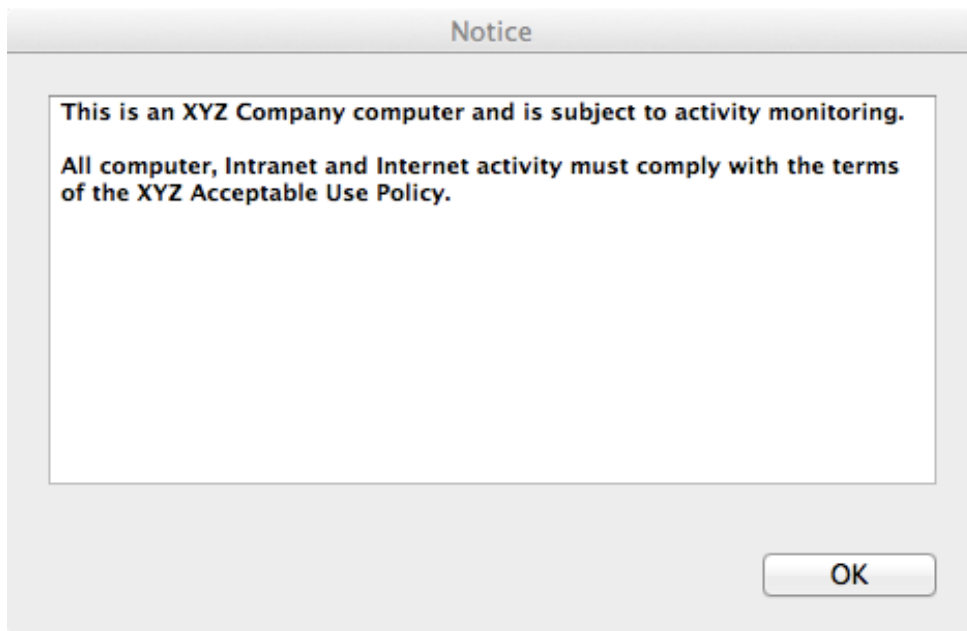
The www.cert.org website is an outstanding resource for insider threat related information.

SpectorSoft

Action Item: Review Your Acceptable Use Policy

If your company does not have an Acceptable Use Policy, now is the time to put one in place. An Acceptable Use Policy ("AUP") serves multiple purposes. It spells out your policies clearly, so that your employees know what is acceptable or not. In this document, you disclose that the organization has the right to monitor activity on company provided devices and on the company network.

Make sure all employees receive a copy your AUP, and acknowledge that receipt – either in writing during their onboarding, or more ideally every time they logon via a click through.
A sample Acceptable Use Policy is included at the end of this document

Notice

This is an XYZ Company computer and is subject to activity monitoring.

All computer, Intranet and Internet activity must comply with the terms of the XYZ Acceptable Use Policy.

OK

1

Spector 360 can be installed as "visible" to the user, appearing as a red icon on the desktop.

2

It allows displaying a custom message every time users log on.

Disclose Means of Monitoring?

It's up to you whether or not to disclose the means by which you monitor. Some companies do, others believe that disclosing the means can lead to employees seeking ways to get around the monitoring, and so choose not to.

The two relevant federal laws in the US to review prior to publishing your AUP are the Electronic Communications Privacy Act of 1986 ("ECPA") and the Computer Fraud and Abuse Act.

The ECPA has two relevant titles – Title I is the Wiretap Act, and Title II is the Stored Communications Act. Both include Consent and Course of Business exemptions.

A few states have laws that require disclosure of monitoring – Connecticut and Delaware were the first to pass this type of law. Colorado and Tennessee have laws specifically regarding the monitoring of public sector employees.

As a best practice, disclosure is recommended whether local law requires it or not. The disclosure can be as high level as "The Company has the right to monitor all activity and communications that take place on company owned computers, devices, and networks" or as detailed as you choose to make it.

SpectorSoft

Decision Point: Consider Involving Your Employees

Your employees are invested in your success and want to contribute to it. Of all companies that are victims of fraudulent activity, 91% incur financial loss, and the typical company loses 5% of its revenues to fraud.* Employees will feel the negative impacts of successful insider threat activity in the form of lower salaries, and potentially even loss of employment.

Consider having employee representation in the meetings where you are weighing the proactive decision. If your goals are clearly articulated, you may find more support than expected - especially if you do a good job of balancing the needs of the company with employee privacy.

## Needs of the Company vs. Employee Privacy

Every organization needs to determine the right balance between the needs of the company and the privacy of their employees. Remember, the vast majority of employees have the companies best interests in mind. Remember, too, that many policy violations and internal security problems are the result of inadvertent mistakes, or lack of knowledge of what is expected or allowed. Just because you took the time to craft an AUP, and your employees have acknowledged it, doesn't mean they've committed it to memory, or even read it.

To strike a balance that's right for your organization, you need options.
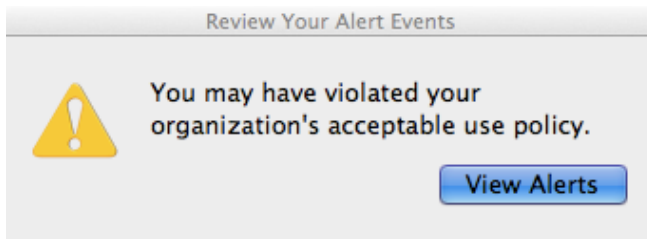
**1** Spector 360 can notify users privately when they trigger alerts, allowing self-correction.
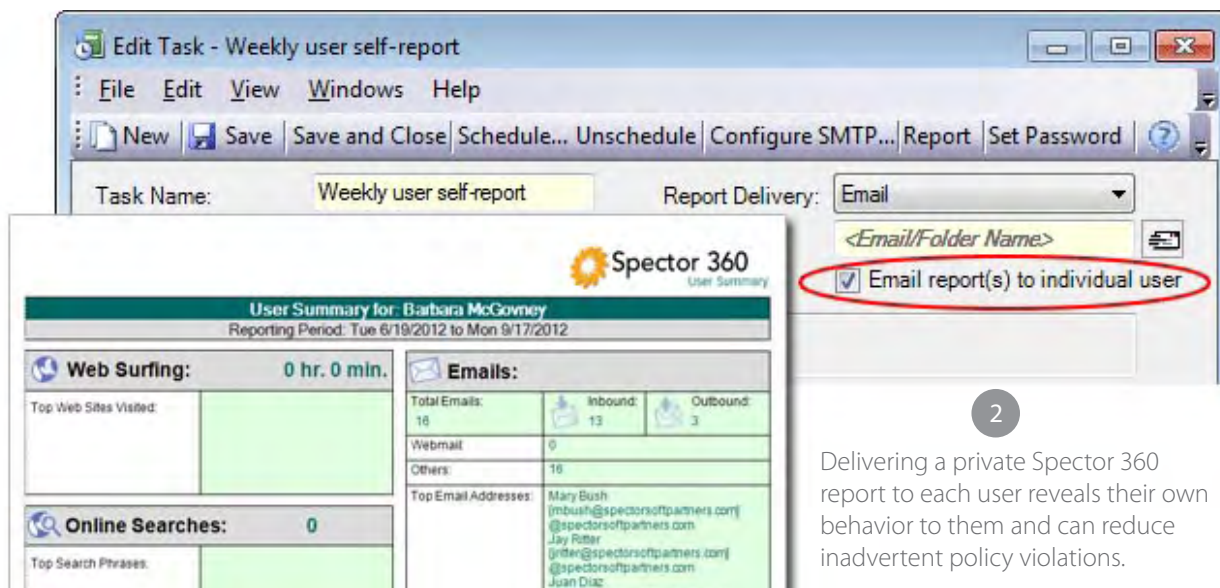
2 Delivering a private Spector 360 report to each user reveals their own behavior to them and can reduce inadvertent policy violations.

* ACFE Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study

SpectorSoft

Decision Point: Active, Passive or Both?

Active Monitoring

An active employee activity monitoring solution records employee digital activity, making the collected data available for review, reporting, and retention. Active monitoring, sometimes referred to as employee surveillance, is typically employed where there is cause to do so.
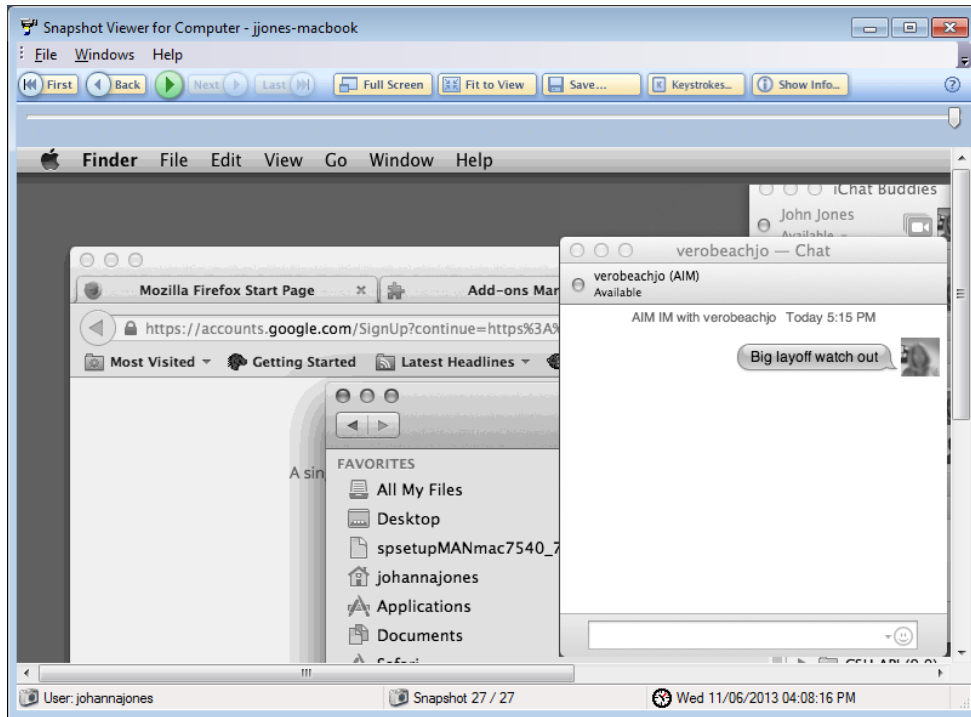
1

Active monitoring in Spector 360 provides screen playback and detailed logs of every user activity.

Cause for active monitoring includes:

Investigatory Cause

Similar to probable cause in the criminal justice world, Investigatory Cause exists where there is a reason to suspect an employee or group of employees is engaging in behavior detrimental to the interests of the organization.

Role-Based Cause

Some positions within the organization have elevated privileges, with the ability to access information that would otherwise be off limits for their functional role. System Administrators and Database Administrators are two examples of highly privileged users (sometimes referred to as "super users"). The definition of an insider threat is use of authorized access in an improper way. Given the disproportionate amount of damage that can be caused by a highly privileged user, many companies apply significant scrutiny to the activities of users in these roles.
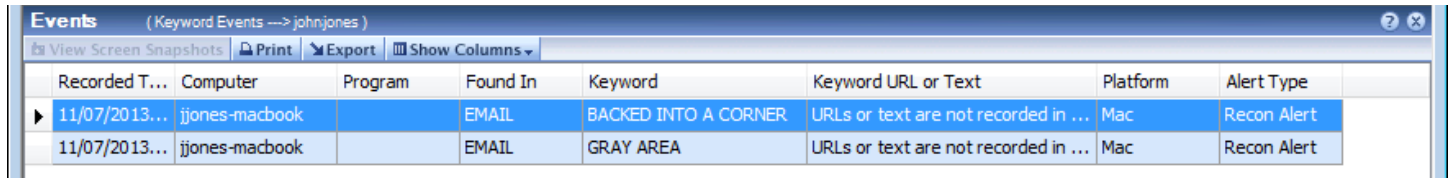
Conditional Cause

Numerous studies, along with research by the highly respected CERT Insider Threat Center, teach us that employees leaving an organization, whether by their choice or by the organization's, take Intellectual Property and other proprietary corporate information with them when they leave. This is a prime example of Conditional Cause – a condition, or situation, exists that requires additional protections be put in place.

SpectorSoft

Passive Monitoring

A passive employee activity monitoring solution records employee activity and generates alerts from events detected in the employee activity logs, but does not make the data collected available for review, reporting, or retention unless there is cause to do so.

The alerts generated by a passive monitoring solution must be configurable so you can focus on activity you are interested in. For example, phrases like "it's off the books" or "it's a gray area" that are used in communications by accounting staff may provide cause for investigating possible employee fraud.
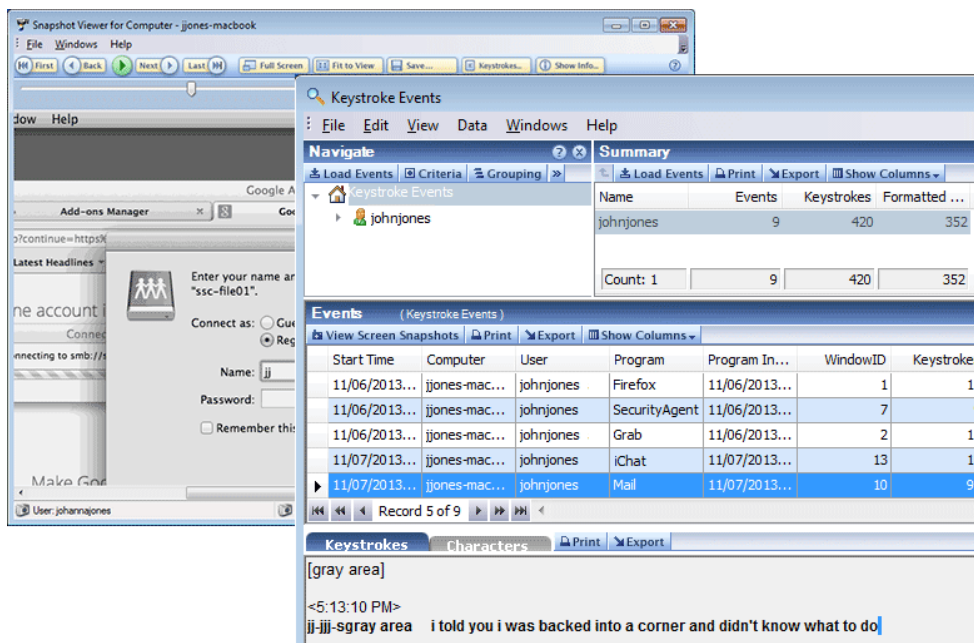

1

Spector 360 Recon watches passively for potential problems. "Events" will appear only if an alert is triggered. Other user activity is not available for viewing.

The Right Mix

Some organizations will determine that passive employee activity monitoring is sufficient to accomplish their goals. Others will determine that a mix of passive and active monitoring makes sense for them — combining broad deployment of the passive capability with targeted use of the active monitoring capability as needed. Finally, some organizations, seeking to receive the maximum benefits from their employee monitoring strategy, will broadly deploy an active monitoring solution.

As you determine which mix is right for you, you are beginning to define requirements for a solution and the characteristics you are looking for in a provider.

2

When there's cause, you can unlock Spector 360 Recon and upload 30 days of screenshots and detailed activity to see exactly what happened.

SpectorSoft

Decision Point: What to Monitor?

The goals you have for monitoring should dictate which employee activities are monitored. Employee privacy concerns usually revolve around some very specific employee activities, such as visiting personal websites or sending personal email.

For example, if you were concerned about what is being done by employees with access to sensitive data, you would want to monitor program activity and track documents. If you have productivity concerns, you might want to monitor websites visited and applications used.

Privacy of Personal Activity

To maintain employee privacy, you can take simple steps, such as not recording your employees' online banking sites or an HR portal where personal information is visible. By aligning what you monitor with your goals, you can achieve them without unduly compromising privacy.

Privacy of Passwords

Unless one of your goals is monitoring for improper use of someone else's credentials, most monitoring of employee activity is about what they access and what is done with data, rather than the credentials used. Look for a solution that gives you the option to capture or not to capture things like personal web passwords. There may be times that capturing a password is necessary, but it is not necessary all the time.

Spector 360 provides an option to mask out passwords

```
<10:22 AM>
florence52   ****************
```

SpectorSoft

Decision Point: Retention and Storage

Now that you have determined how (active, passive or both) and what to monitor, you need to decide how long you retain the collected information, and where it is stored.

How Long?

Companies that employ passive monitoring typically retain the recorded data for a short period of time. These companies are interested in having enough data to determine what happened before, during and after an alert or other trigger – but do not wish to maintain an archive of employee activity.

Companies engaged in active monitoring are typically interested in maintaining a longer record of employee activity. Make sure the solution you select allows you flexibility in defining the retention period.

Where?

Where the data is retained is another key decision point. Some companies prefer the employee computer activity log to be kept locally, and securely, on the machine where the activity occurred. This approach is aligned with a passive monitoring strategy.

Others prefer to store the data in a central database for retention and backup; companies engaged in active monitoring are more likely to fall into this category.

A well thought out monitoring solution provides storage options.

Decision Point: Alerts, Escalation and Review

Finally, establish review and escalation procedures. Just because IT is essential to the evaluation and implementation of your chosen solution does not mean you have to task them with reviewing all of the data. Determine who in your organization should have access to the employee activity data, and under what circumstances.

Who Receives Alerts?

Here again, your goals and organizational structure will inform your decisions. If you are passively monitoring sales and accounting for signs of employee fraud, you may want alerts on potential fraudulent activity to go to the office of the Chief Financial Officer. If you are monitoring for indications of inappropriate workplace behaviors, like sexual harassment, you will want Human Resources to receive relevant information. You may also want to educate your employees to violations of your Acceptable Use Policy as they occur, to reinforce your policies and to help modify potentially problematic behaviors.

Issues like IP Theft would be referred to IT Security or Incident Response teams, or the equivalent roles in your organization.
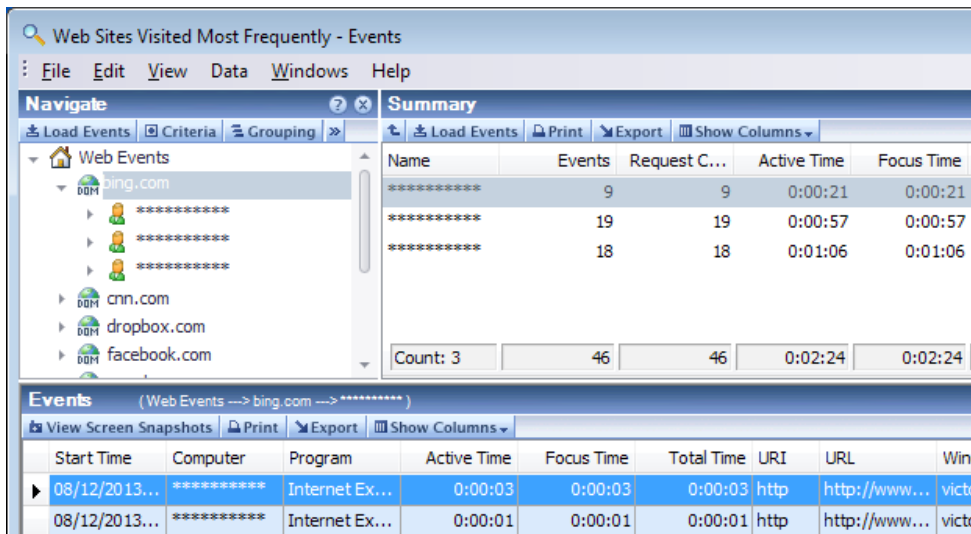
As a general rule, alerts should be routed to the experts in your company who are in the best position to determine the severity of a potential problem, so that the appropriate response can be formulated.

SpectorSoft

Who Reviews Activity?

One of the compelling benefits of employee activity monitoring is that review of what was done, by whom, and in what context, can be conducted quickly, accurately, and efficiently. This does not mean that review should be taken lightly, however, or that "anyone can do it."

Perhaps the most important decision you will make is determining who has the ability to review detailed employee activity records.

In situations where active monitoring is being conducted, the review processes and procedures are in use continuously. A look back at the "causes" for active monitoring is useful here:

1

Spector 360 provides user access controls to determine who views what data. Additionally, user names can be masked out in activity.

Investigatory Cause

In the event of an investigation into a suspected incident, your company's employee investigation procedures go into effect. Who can initiate an employee investigation? Who needs to be informed that an investigation is needed? Starting? Concluded?

A best practice for companies conducting passive monitoring, that have determined sufficient probable cause exists to warrant tilting the balance from employee privacy towards the needs of the company, is to employ a "two missile key" approach. Require at least two approvals prior to kicking off an employee investigation – ideally one from HR or Legal, and the other from a senior manager or their designee. Split the ability to access the employee activity data into two pieces as well, to insure proper procedure is not circumvented.

Role-Based Cause

Using the same highly privileged user example referenced earlier, consider having regular, random, reviews of sys admin or database admin activity conducted by someone outside of the IT chain of command (your CISO, for example), if your company structure allows for it. If that is not an option, have the most senior person in your organization that is directly responsible for protecting the company's data and sensitive information conduct the reviews. The disproportionate amount of damage highly privileged users can cause requires a proportionate amount of scrutiny be applied.

SpectorSoft

Conditional Cause

Given the powerful statistical evidence that departing employees take corporate IP with them when they leave, having IT security or Human Resources reviewing the digital activity of employees in this high risk exit period is prudent.

Action Item: Ensure Adherence to Policies and Procedures

Whatever policies you put in place, make sure you are auditing compliance with those policies. And make sure you select a solution that supports that need. By having controls in place that both prevent changes from being made by unauthorized personnel and log (and alert on) any changes made, you gain the piece of mind that your controls are not being circumvented, and the ability to confidently assure anyone who may have concerns that you've taken appropriate steps to implementing employee activity monitoring the "right way."

Sample Acceptable Use Policy

Click here to download a recommended outline of the components and characteristics of an Acceptable Use Policy template. We recommend that your Legal department review and make any necessary changes.

Corporate Offices

SpectorSoft Corporation

1555 Indian River Drive

Vero Beach, FL 32960 1.888.598.2788

Toll Free Phone/Support 24/7

1.772.770.5670

West Palm Beach

1555 Palm Beach Lakes Blvd.

West Palm Beach, FL 33401

International

United Kingdom

C2, Dukes Street

Woking

Surrey, GU21 5BH

+44 1483 397744

SpectorSoft