Wavecrest

EMPLOYEE WEB-USE MANAGEMENT IT'S A PEOPLE ISSUE

The

HUMAN FACTOR

White Paper Series

www.wavecrest.net

Executive Summary

Written primarily for Human Capital or HR professionals, but also useful to all managers, this paper discusses employee Web-use management, that is, the process of ensuring that workers use the Web, also commonly referred to as the Internet, for productive, work-related purposes only. The discussion explores the subject from several perspectives and underscores the following points:

- *Employee Web-use management is a people issue, not just an IT issue.*
- *Because it is a people issue, HR personnel should take the lead in proposing and developing solutions to ensure that the human factor is properly managed.*
- *Employee Web-use management is a way for HR to contribute to the engagement, productivity, network security, and profitability of the organization.*

The paper begins with a discussion of Web use in the workplace for nonwork-related purposes as well as business purposes. If unauthorized, this activity can degrade workforce productivity, impact network performance, threaten network security, and create legal liabilities. Any of these outcomes can seriously impact the organization's bottom line. Effective employee Web-use management programs are essential to prevent this from happening, but they need to be implemented without degrading workforce engagement and morale.

Because this subject deals with human behavior in the workplace, the paper discusses why HR personnel are the professionals best equipped to take the lead in developing and implementing employee Web-use management efforts, collaborating as required with executive management, functional managers, and IT personnel. The paper then examines the main elements of an effective employee Web-use management program, that is, Web-access policy, training, and compliance. Implications for workforce morale are explored as well.

Also discussed is the availability of Web-use management software tools that can help in the effort. These tools can provide Web-access reporting for HR which is a key element in the overall solution, as well as a combination of Web-access reporting and filtering to monitor policy compliance and control Web access. They need to be chosen carefully to ensure accuracy, effectiveness, and flexibility. Although effort is required, the employee Web-use problem can be successfully managed with proper HR and management attention to the benefit of the enterprise.

Introduction

The need for employee Web-use management and security is a must in most workplaces because of the tremendous increase in surfing the Web at work. Employees shop, do online banking, visit sports sites, use Facebook, and more on the Web, spending between one and three hours a day on personal business at work. Employees also deploy cloud applications that help them do their jobs more quickly and easily; however, not all employee-introduced cloud services are authorized. Because of the Internet's relationship to technology, it is mistakenly believed that Web-use management is an IT issue, one that can somehow be solved with user IDs, passwords, firewalls, and so on. This is simply not the case. It is a people issue, one that involves human behavior in the workplace.

Employees can choose to visit certain Web sites for productive, work-related purposes, or they can choose to visit other sites for nonproductive, personal purposes. They may not even know what types of visits are appropriate or inappropriate in the workplace. Employees can be subject to phishing scams and bogus Web links. In addition, they may or may not work in an atmosphere that prohibits inappropriate

use of Web-access resources, and by lack of training or awareness, they may inadvertently end up on malicious Web sites where hackers lie in wait for unsuspecting visitors. And finally, employees may not have a clear-cut Web-usage policy to guide their online behavior.

> "People open 3% of their spam and 70% of spear-phishing attempts. And 50% of those who open the spear-phishing emails click on the links within the email—compared to 5% for mass mailings—and they click on those links within an hour of receipt. A campaign of 10 emails has a 90% chance of snaring its target."
>
> —FireEye

For all of these people-oriented scenarios, there is a clear need for HR personnel to take the lead in developing and implementing an effective employee Web-use management program. This is the focus of this paper with subsequent sections discussing the background of the problem, who should be responsible for resolving the problem, and the kinds of efforts required to implement a solution to the problem.

Background of the employee Web-use problem

As mentioned above, there has been a significant increase in Internet use in the workplace. From a business perspective, there are many valid reasons for workers to have this access, for example, to perform important business processes and research tasks. Such access can and does contribute much to the agility, efficiency, innovativeness, and success of the enterprise. And with the number of cloud applications and services that businesses depend on, Web access has become more and more integral to the performance of core enterprise functions every day.

On the other hand, Web access has significant, potential, negative consequences. According to an IDC White Paper, data generated worldwide is at over 16.1 zettabytes (1 zettabyte = 1 trillion gigabytes). Access to this data deluge has fostered an atmosphere of productivity loss and increased "me time" entitlement. Employees can waste considerable work time and network resources accessing various sites for personal reasons. Wasted time obviously represents a reduction in productivity and efficiency and thus unnecessary cost.

> According to a CNBC article, Mark Zuckerberg founded Facebook with a simple dream: to have everyone spending as much time as possible clicking around on his Web site. In early 2016, the social network site's users were closing in on $3.5 trillion in squandered productivity, and the company has about 1.6 billion monthly active users, more than the population of any single country on earth.

Employers also have concerns about where their employees are surfing the Web at work. Unfortunately, one of the most serious forms of Web-access abuse involves the downloading and displaying of pornography. Such activity not only detracts from workforce productivity, but is a human factor vulnerability that can lead to legal liabilities, primarily in the form of sexual harassment lawsuits. Typically, such suits are filed by employees who have inadvertently or deliberately been exposed to pornographic images downloaded by other employees. In one company, IT became suspicious by the change in position of an employee's computer, making the view of the screen impossible by anyone except the employee. They found that the employee was downloading and watching pornographic movies.

> Another distraction that is a huge issue from the standpoint of workplace liability is pornography viewing at work. Nielsen has found that 25 percent of working adults admit to looking at pornography on a computer at work. And 70 percent of all online pornography access occurs between 9 AM and 5 PM.
>
> —Forbes.com

Included in the employee Web-use problem is the prevalence of malware which is a major concern. Employees can be tricked into going to a hacked site and then downloading an infected document. Since malware most times requires that they proactively click a link or button, clicking prompts such as “Enable Editing” and “Macros have been disabled” in a Microsoft Word document for example, will infect their system. Employees need to be trained to pay attention to what they are clicking on, not enable macros, or open unknown attachments.

Additionally, employees can waste time on legitimate but unproductive Web site visits. Such waste can stem from flawed business strategy, poorly designed processes, faulty managerial decisions, or misguided supervisory direction. Such misuse can represent missed profit opportunities and degrade corporate ROI.

Managing employees’ use of Web-access resources is a sensitive and complex task, one that deals with policy, training, and compliance issues, and one that is crucial to productivity, profitability, and morale in the workplace. Serious and informed managerial leadership is required as well as a well-organized and multifaceted program.

Who is responsible for employee Web-use management?

The preceding section points out why every organization that provides Internet access to its employees needs an effective employee Web-use management program. However, as with any other major management issue, the following questions may arise: Who is or should be responsible for developing, implementing, and managing the program? Isn’t Web-use management and security an IT issue?

Web-use management and the role of IT

As mentioned earlier, many people think that Web-use management is an IT issue, one that can and should be solved by IT personnel. But, as also pointed out earlier, the fundamental problem is a people issue, one which IT personnel typically are not suited for, by virtue of training, experience, resources, and long-standing traditional responsibilities. Typical IT responsibilities and capabilities are as follows:

- IT is responsible for providing a secure infrastructure and protecting company data, but they are not responsible for how resources are used functionally on a day-to-day basis. For example, IT can give you Microsoft Office 365, but they cannot control how you use it.
- IT is responsible for solving technical problems. Web-use management is not a technical problem; it is a people problem.
- IT can deploy firewalls and network security equipment, but is not equipped or trained to deal with the larger issue of keeping the trusted workforce from compromising the well-thought-out and well-placed security measures implemented by IT.

So while IT can provide some technology to help out, they are not in a position to design, implement, and manage an overall employee Web-use management program.

Employee Web-use management is a team effort led by HR

An effective employee Web-use management program will involve multiple areas of the organization. Consequently, and ideally, employee Web-use management should be a team effort involving five groups:

- **Human Resources Personnel** - HR is best equipped to take the lead, initiate policy, suggest tools and processes, and orient and train employees.
- **Senior Management (CEO and senior division managers)** - Senior management needs to provide overall guidance, approve policies and processes, establish corporate culture, support HR and IT efforts, and stay involved.
- **Information Technology Personnel** - IT personnel can help evaluate, select, install, and set up software tools. They can also share with HR the ever-changing types of attacks trending on the Web and ways to help employees avoid them.
- **Department Managers and Supervisors** - Managers and supervisors need to use reports, counsel employees, recommend blocking regimes, stay involved, and follow up.
- **Individual Users (Employees)** - Individual users should know the policy, and use Internet and intranet access properly, not for personal purposes. They should also know how to recognize online threats and how to report them.

While all five of these groups are important, leadership by HR is particularly critical.

Leadership by Human Resources

As indicated above, Web-use management is not just an IT issue. It is all about employee behavior, productivity, and morale, and its resolution involves matters of policy, training, and compliance. Because HR departments are accustomed to dealing with similar or related matters, they are in the best position to take the lead in instituting an effective employee Web-use management program to ensure that the human factor is properly managed. HR's expertise typically includes personnel policy, codes of conduct, labor relations, workforce training, legal compliance issues, and workforce morale, all of which relate to the employee Web-use management issue.

In addition, by virtue of their personal backgrounds, orientation, and job responsibilities, HR personnel are in the best position to be objective in this sensitive area. Objectivity and evenhandedness are necessary to strike an optimum balance between overly rigid controls on the one hand and total laxity on the other. By taking the lead on this issue, HR personnel can:

- Make a positive contribution to workforce productivity and organizational profitability.
- Play a key role in proper network resources and policy training that would have a significant impact on corporate Web security.
- Help keep the company out of severe legal difficulty.
- Help maintain or improve workforce morale.
- Ensure a balanced approach to Web-use management.

> Workers said they waste time by: surfing the Web (48%), socializing with coworkers (33%), conducting personal business (30%), making personal phone calls (19%), and taking long lunch breaks (15%).
>
> —HRMorning.com

Specific role of HR

To ensure successful and effective employee Web-use management, HR's role will need to include the following tasks:

- Educate senior management on the importance of employee Web-use management, get their input, and keep them involved.
- Establish a sound Acceptable Use Policy (AUP) consistent with the company's culture.
- Communicate the policy to the workforce.
- Establish Web-use training programs for managers and employees.
- Work with functional managers and IT to ensure optimum implementation.
- Revise Web-use policies when experience dictates.
- Stay abreast of related legislation and litigation.
- Follow up and stay involved. Work with functional managers on specific cases.
- Utilize Web reporting and blocking tools that are reliable and accurate.

Informed and motivated HR professionals can do these tasks well in the framework of a well-designed Web-use management program. The next section describes the elements of such a program, one that can go a long way toward ensuring optimum use of Web access in the workplace.

An effective employee Web-use management program

The previous sections pointed out why an effective employee Web-use management program is essential to today's businesses and who should be responsible for leading its design and implementation. This section provides a summarized analysis of such a program. The analysis recognizes that the specifics will vary from business to business in accordance with corporate culture and management style.

Definition of employee Web-use management

Employee Web-use management is the continuous process of ensuring that workers use Web access for productive, work-related purposes only. At a conceptual level, it can be likened to other areas of personnel management such as:

- Controlling personal smartphone calls in the workplace.
- Controlling and preventing employee theft of company property.
- Policies to maximize productivity, for example, limits on lunch and other breaks.
- Controlling use of company property for personal use, for example, vehicles and copiers.
- Labor cost distribution reporting to track how resources are being used.
- Use of employees' code of conduct concerning ethics and integrity in the workplace.

Requirements of an effective program

To be effective, employee Web-use management requires that responsible HR personnel and other management personnel conduct five activities:

1. Develop a sound AUP consistent with corporate culture.
2. Communicate that policy clearly to all users informing them of what is and what is not acceptable.
3. Train employees on how to use Web access productively and safely.
4. Use reliable software tools that are designed specifically to monitor compliance with Web-use policies and proactively control Web access.
5. Follow up with corrective actions when inappropriate access is detected.

If these responsibilities are carried out well, misuse and abuse of network resources will be minimized without damaging workforce morale. These five activities are discussed below.

1. Acceptable Use Policy

As mentioned above, a crucial and prerequisite component of an effective Web-use management program is a carefully crafted AUP. Fundamentally, the AUP spells out in writing what type of Web-access activity is acceptable, what type is not, and the consequences of engaging in the latter. An effective AUP will be clear, detailed, unambiguous, and reflective of the corporate culture.

Most importantly, the AUP should include ground rules and standards for what constitutes desirable, acceptable, unacceptable, and abusive use of the Internet and other network resources. In other words, the policy and rules must address the question: For our particular enterprise and for specific departments and individuals within the enterprise, exactly what constitutes legitimate, productive use of the Internet and what constitutes abuse?

Depending on the corporate culture, some activity may be defined as acceptable usage even if such usage is not for business purposes. For example, a few minutes to check the stock market or sports scores during the lunch hour may be perfectly acceptable and may be conducive to good morale, but exceeding the limit may be abusive. This provision enables the enterprise to permit and control limited use of network resources for personal or morale reasons.

The policy should also state clearly how compliance will be monitored and what the consequences will be to the individual abusing the use of network resources. In sum, the policy needs to be carefully crafted, well-defined, precise, and reasonable. It must also be specific to the enterprise, easily auditable, and clearly communicated to all concerned in easily understood language.

There are several reasons why well-designed AUPs are so important:

- People work best when they know the rules.
- Rules serve as the baseline for gauging acceptability.
- Rules can be built into monitoring and control tools, such as category ratings, abuse thresholds, and access denials.
- Reasonable rules encourage appropriate behavior and discourage inappropriate behavior.
- Clear policies minimize, if not eliminate, the necessity of management intervention.

- Workers will be demoralized by enforcement of unstated or unclear policies.
- Employees will be aware of avoiding unknown Web sites and accessing only known, trusted sites.

2. Communicating the policy to all concerned

The policy should be provided in writing to all concerned. This includes management personnel as well as the general workforce. All recipients should be required to sign and return a copy of the policy to HR, indicating that they have read and understand its contents. HR and management personnel should hold meetings with workgroups to answer questions and provide additional information.

3. Training the workforce on the use of network resources

In addition to communicating the policy to all concerned, HR and management personnel should conduct broader-based training sessions covering Internet usage and related subjects. Specifically, employees need to be made aware of what sites they are visiting and what they are clicking on the Web. The purpose should be to encourage proper, productive, and safe use of network resources while reinforcing the information in the AUP.

> Concerning employee privacy and workforce morale issues, some people might view employee Web-use management as a violation of privacy. However, courts have ruled consistently that employers have a right to ensure that their property and resources are not being stolen or used improperly by employees. Competent management can prevent damage to morale by employing enlightened, open, analytical approaches. These include implementation of a reasonable and rational policy, clear and honest communications, and reliable metrics.

4. Using Web-use management software tools

Having published a sound AUP and trained the workforce in proper use of network resources, management now needs to monitor and control actual usage. Software tools can help with this part of the program. Basically, software can perform the following functions:

Monitor and report on Web usage

Software is available to monitor compliance and ensure conformity with the organization's AUP. The software should be configured to do its job in a constructive and reasonable manner. In addition to reporting, such monitoring can and should identify positive, desirable Web usage as well as negative trends and unacceptable use. By keeping track of employees' efforts in this way, leaders will get to know their people better, give more effective direction, and motivate their workforce. They will also be able to keep projects on track, boost productivity, and correct mistakes before they turn into serious problems.

Control access to specified Web sites

Software is also available to selectively filter users' access to designated Web sites while allowing access to other sites. Sites that can be filtered are those in totally unacceptable categories such as those related to pornography, illegal drugs, and hate/crime. Also sometimes included are categories that might be considered inappropriate, for example, games, sports, shopping, social media, and chat.

With respect to the selection of tools, management should insist on software that:

- Was developed from the ground up for managing human behavior, not for tracking bits and bytes, that is, what is needed is an HR tool, not an IT tool.
- Was developed solely for outbound reporting and control and is not an adaptation of a tool developed for inbound reporting.
- Differentiates true visits (clicks initiated by human action) from extraneous or irrelevant hits. This feature is necessary to accurately interpret employee behavior. For more information, see the white paper in the Human Factor series that discusses understanding behavioral analytics with reliable metrics.
- Counts clicks to measure the extent of activity.
- Uses a broad-based URL list that does not focus on just legal liability sites.
- Was developed by a firm that specializes in Web-use management and security across the board, not just prevention of legal liability.
- Is furnished by a vendor that provides complete and effective follow-on support.
- Provides information that is actionable, reliable, and accurate.

With reference to the last item in the above list, high levels of accuracy and reliability are essential to ensure that:

- Employees are not falsely accused of Web-access abuse.
- Managers reach sound, valid conclusions when assessing Web-use activity.
- Managers make well-founded decisions and take appropriate corrective action.
- Different managers and departments make consistent interpretation of results.
- Policy enforcement is consistent from department to department.
- Management stays on solid ground legally.
- The morale of the workforce is not damaged.

5. Management follow-up action

With a policy in place, personnel oriented, the workforce trained, and software busily monitoring and controlling Web usage, there is still much to do. The software will inevitably reveal patterns of inappropriate use or disclose signs of outright abuse. These will all require attention by HR and/or management personnel.

After identifying the problems, management can take appropriate follow-up actions, such as counseling employees, training or retraining workers, changing work processes, and revising or clarifying the AUP. Managers may also need to institute follow-up audits on individual users and, in worst case, take disciplinary action including termination.

Conclusion

Employee Web-use management is a people issue, not just an IT challenge. It deals exclusively with human behavior in the workplace and is a complex, never-ending management challenge with serious implications for the business's bottom line. It must be constantly pursued in a firm, but fair manner. By virtue of training, experience, temperament, and mission, HR personnel are the best equipped to take the lead in implementing a firm, but fair employee Web-use management program.

The objective of such a program should be to capitalize on the beneficial, productive potential of Internet access while precluding or minimizing its negative aspects. The challenge is to achieve this objective in a balanced way, one that fosters and promotes the interest of the enterprise as a whole without creating an oppressive "Big Brother is watching you" climate in the workplace. This is a delicate balancing act, one that is not easy to define and achieve. Recognition of the following will help:

- It is all about the human factor, that is, people and their behavior.
- Inappropriate and improper use of the Internet in the workplace is a critical and potentially costly issue.
- The biggest Web-use problems stem from human nature and the size and rapid growth of the Web.
- Web-use management is not a technical or IT issue, and it cannot be solved with technology alone, although IT personnel and technology tools can help.
- Highly accurate tools are essential to the success of the program. Such tools are designed from the ground up for monitoring human activity, not for tracking bits and bytes.
- Employee Web-use management deals with issues of policy, training, and compliance, and good communication is critical to all three.
- HR personnel are best equipped to take the lead in Web-use management efforts.

Effective Web-use management and security can be a real challenge, and there will be hurdles along the way. Along with HR personnel, managers need to become considerably more involved in planning and controlling Web usage by developing and implementing policy-based Web-use management approaches. The next paper in the series will discuss proactively managing Web use with the human-based policies of a Web-use management product.

About Wavecrest Computing

Wavecrest has over 20 years of proven history of providing reliable, accurate Web-use management and Advanced Log File Analyzer products across various industries. Managed Service Providers, IT Specialists, HR professionals, Forensics Investigators, and business managers trust Wavecrest's Cyfin and CyBlock products to manage the human factor in business Internet usage–managing cloud services, reducing liability risks, improving productivity, saving bandwidth, and controlling costs. Wavecrest is trusted by large government and commercial organizations such as US-CERT Homeland Security, U.S. Department of Justice, USPS Office of Inspector General, National Grid, Johns Hopkins, and a growing list of global enterprises and government agencies. We are a proud long-term GSA contract holder. For more information on the company, products, and partners, visit https://www.wavecrest.net.

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350