Realtime publishers
"Leading the Conversation"

The Essentials Series:
Email-Centric Data Loss Prevention

Employees' Role in Data Loss Prevention

sponsored by

proofpoint

by Dan Sullivan

Copyright Statement

Employees' Role in Data Loss Prevention

Effective data loss prevention (DLP) strategies leverage a combination of technical controls and employee understanding of DLP policies. In this, the second article in the series, we focus on the role of employees in protecting information assets. Employees' actions with respect to DLP are guided by policies, so it is imperative that these policies are crafted according to current business requirements and that the policies are understood by employees.

If only one term were allowed to describe effective email policies and training programs it would be "pragmatic." One can imagine draconian measures deployed to ensure that no data is inadvertently disclosed through email, but at what cost? Could business operations function efficiently under such measures? As with other areas of risk management, email policy and employee training must balance the need for security and compliance with the need to support business operations. One of the key challenges in realizing this balance is that email and related communication mechanisms are not static technologies: the way we use them and the rules that govern their use are in flux.

Email Policy and the Real World

If you were to read an email policy written 10 years ago, you might have one of several reactions:

- The policy is naïve and missing requisite mention of commonly encountered issues of today
- The policy is overly restrictive, limiting use of communications systems to strictly business-related operations
- The policy does not account for mobile or remote access
- The policy does not sufficiently describe employers' rights to monitor email
- The policy does not sufficiently describe employees' responsibilities with respect to DLP and other security concerns

The underlying issue is that both technology and the way we use it has changed and continues to change. Email policies must stay in step with these changes.

Email Policy and Technical Advances

Early email systems ran on centralized computers that provided access through attached terminals. There was no concern about distributed access from desktop PCs, mobile devices using public networks, or employee's home computers. Today's email administrators have to contend with all these issues.

Advances in networking, email servers, and email clients allow users to access their email from a wide range of devices. Some of these, like corporate PCs, are managed devices running appropriate security software that is properly configured and patched according to IT policies. We typically have the most confidence in these devices because the risks from these devices are understood and sufficiently controlled.

Personal mobile devices, such as PDAs and smartphones, may be used by employees to access email using public cellular or WiFi networks. When these devices are owned by employees but used for business, there are greater risks. Data leaks can occur in a variety of ways. Employees might not encrypt confidential information, which puts the data at great risk if the device is stolen. Software may not be patched as need to avoid known vulnerabilities. Sensitive data may be transmitted over public, unencrypted wireless networks. There are limits to what a business can reasonably expect to control on personal devices, but today's email policies can specify the types of security measures that should be in place on personal devices before they are used for accessing the corporate email system.

Unmanaged, shared devices can be an IT manager's worst nightmare. These include PCs in hotel business centers, public access computers in convention halls, and even employees' home computers shared with family members with little concern for security (think file-sharing, ringtone downloading teenagers who keep up with the latest browser plugins). Although businesses cannot control how these devices are configured, they can set policies for minimum security and configuration requirements for devices connecting to their networks and servers. The expanding set of options for accessing email presents new scenarios that should be considered in email policies, but it is not just technical changes that demand updates to email policies.

Evolution of Acceptable Use

The phrase "acceptable use" is widely used to describe the kinds of activities that one is allowed to engage in when using corporate IT resources. With regards to email, acceptable use at one time meant strictly business related, at least from the perspective of policy designers. Emailing messages about meetings, project status reports, and application documentation clearly feel within the bounds of strictly business-related. What about a message wishing an employee a happy birthday, asking for volunteers for a local charity, or announcing a social gathering outside of work? These have more to do with employee morale than business operations. Given their importance for building community bonds in an organization, the scope of acceptable use has expanded to include these kinds of messages.

Businesses are also adapting to less clear boundaries between personal and work lives. Fifty years ago, a knowledge worker might bring some papers home during a busy time at the office, but leaving work at the office was more the norm than it is now. Today's technology provides greater productivity outside the office. For example, employees might check their email from home before beginning their commute and call colleagues from their cell phones while on the road. Communications has extended the reach of business into personal lives so much that technology writers are offering tips on how to have a successful vacation while still managing email (see James A. Martin's "E-mail on Vacation" at Yahoo!Tech for more). The same technology that helps employees keep in touch when away from the office also helps us keep up with personal matters while at the office.

Reasonable interpretations of acceptable use now include occasional emails between spouses, between parents and children, and between friends. If personal use does not interfere with work, incur an additional cost on the business, or present security issues, the use would likely be considered reasonable by today's standards.

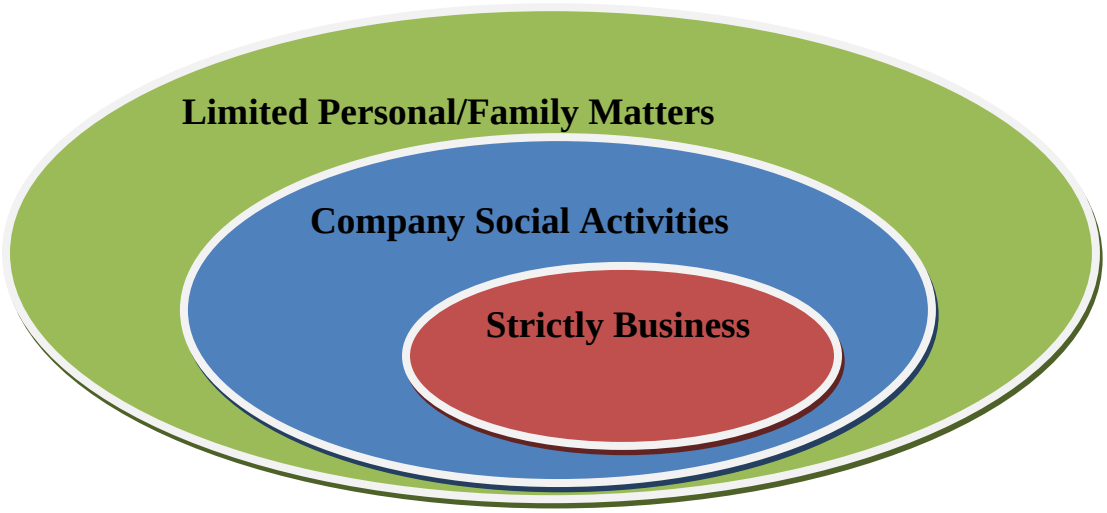

Figure 1: The scope of "acceptable use" has expanded from a strict interpretation of business activities to a broader understanding of supporting reasonable personal needs of employees.

The intertwining of business and personal aspects of employee lives is common in today's corporate environment, and policies alone will not change that. Instead, policies should reflect a balance between the needs of business and the reasonable behaviors and expectations of employees.

Potential Disconnects Between Policies and Today's Environments

Common practices and uses of communication technologies change according business requirements and reasonable personal expectations. This dynamic creates the potential for stagnant policies that do not address emerging issues, including those that arise because of changes in technology and common employee behaviors.

The clearest example in changes in technology that impact email policy is the advent of Web 2.0 technologies. Communications on Web sites is now two-way, with employees able to share information and opinions with a wide audience of friends, colleagues, and complete strangers. These options can supplant email as the communication tool of choice in many situations:

- An employee commenting on a blog about her opinion on the management of a recent merger
- An analyst noting on his Facebook profile that he is working on project for a particular client
- A systems administrator adding a company-specific example to wiki documentation for an open source application used by the company

In all these cases, it could be public information that is shared or it could contain private and confidential details that should not be disclosed. These disclosures are not made via email, so reasonable employees may assume the email policy does not apply. Web 2.0 technologies create potential conduits for data loss, and policies should be in place to explain acceptable use in these cases.

The need for expanding the scope of policies is justified by the widespread use of Web 2.0 technologies and the demonstrated need for DLP measures with existing email systems. Consider some of the findings from Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008*, an international survey of large enterprise responses to and concerns about outbound messaging security (all statistics are for the 12-month period prior to survey). With respect to email:

- 44% of US companies surveyed had investigated a suspected email leak of confidential or proprietary information
- 40% of survey respondents had investigated a suspected violation of privacy or data protection regulations
- 51% of US companies surveyed had disciplined an employee for violating email policies

With respect to Web 2.0 technologies:

- 44% are concerned or very concerned about the risk of information leakage via media sharing sites
- 44% are concerned or very concerned about the risk of information leakage via blogs and message board postings
- 21% investigated the exposure of confidential, sensitive, or private information via a blog or message board posting

Businesses are concerned about abusive use of communications technologies and acting on those concerns with investigations and disciplinary actions. Although fewer survey respondents have investigated blog and message postings than ultimately disciplined employees for violating email policies, the number of blog and related investigations is likely to rise. Rather than waiting for significant increases in these incidents, companies can stem potential incidents by updating employee education programs.

Employee Education and DLP

Employee education begins with a baseline set of information that employees should know. This includes a reasonable definition of acceptable use. Again, this term has evolved and the definition should reflect an understanding of the needs and expectations of the business along with consideration of how many employees balance the needs of work and family. Policies should address multiple modes of communication, including email, blogs, message boards, social networking sites, wikis, and other collaborative information-sharing tools. This could help to reduce the kinds of violations that led 26% of surveyed U.S. companies to terminate employees for violating email policies and 51% to discipline employees for such violations.

An extension of this kind of comprehensive policy is to focus on educating employees about information classification. For example, companies divide information into four categories:

- Public information, which is information that can be shared with anyone outside the company without harming the company, its customers or business partners, such as memos on building maintenance or changes in parking policies.
- Sensitive information, which is information that is not generally available to the public but if disclosed would not harm the company, its customers, or business partners; examples include project status reports, employee time sheets, or approved vendor lists.
- Private information, which is personal information provided by customers, clients, or patients and kept in confidence by the company; Social Security numbers and healthcare information fall into this category.
- Confidential information, which is information that if released could harm the business; trade secrets and unpublished financial results are examples of confidential information.

Again, the need for this kind of education is illustrated by findings from Proofpoint's 2008 survey, which found 14% of US publicly-traded companies and 11% of European publically traded companies surveyed had investigated exposure of material financial information on a blog or message board. Data from the survey provides an aggregate view of the state of email security and DLP concerns, but it is also important to understand the particular needs of individual businesses.

Understanding the Specific Needs of Your Organization

Automated DLP tools can not only enforce policies on outbound content but also collect valuable data about the types of policy violations, where in the company they are occurring, and the frequency of violations. This kind of raw data can help IT and HR personnel to identify parts of policies that may not be clear or weakness in training material. This in turn will allow more targeted training and faster response to incidents.

When automated monitoring is in place and employees are aware of it, there may be a more subtle benefit: avoiding the "broken window" phenomenon that can occur when there is a perceived lack of authority and no penalties for violations, which in turn leads to further harm. (This phenomenon has been seen in project management; see Gary Petersen's "Broken Window").

In summary, employees play an essential role in email-based DLP, and their success depends, in part, on comprehensive policies that are up to date with the way employees work, communicated through effective training, and enforced with automated tools.