AMA/ePolicy Institute Research

2006 WORKPLACE E-MAIL, INSTANT MESSAGING & BLOG SURVEY

EXECUTIVE SUMMARY: E-MAIL RISKS & RULES, POLICIES & PROCEDURES

E-mail mismanagement continues to take a hefty toll on U.S. employers, with costly lawsuits—and employee terminations—topping the list of electronic risks.

As recent court cases demonstrate, e-mail can sink businesses—legally and financially. In 2005, the inability to produce subpoenaed e-mail resulted in million dollar—even billion dollar—lawsuits. In fact, 24% of organizations have had employee e-mail subpoenaed (versus 20% in 2004), and 15% of companies have gone to court to battle lawsuits triggered by employee e-mail (up from 13% just two years ago).

Increasingly, employers are fighting back by firing workers who violate computer privileges. Fully 26% of employers have terminated employees for e-mail misuse. Another 2% have dismissed workers for inappropriate instant messenger (IM) chat. And nearly 2% have fired workers for offensive blog content—including posts on employees' personal home-based blogs. In 2005, when AMA and The ePolicy Institute surveyed electronic monitoring and surveillance policies and practices in the workplace, 25% of employers reported firing employees for e-mail misuse, and another 26% said they had terminated workers for Internet violations.

FINDINGS: WORKPLACE E-MAIL

Q. Does your organization have a written policy governing e-mail use and content?

Yes 76%

Q. Does your organization formally train employees about e-mail risks, policy and usage?

Yes 42%

Q. Has your organization ever been ordered by a court or regulatory body to produce employee e-mail? (In other words, has employee e-mail ever been subpoenaed?)

Yes 24%

Q. Has your organization ever battled a workplace lawsuit triggered by employee e-mail (sexual harassment/discrimination; racial harassment/discrimination; hostile work environment claim; any other claim)?

Yes	15%

Q. Has your organization ever fired an employee for e-mail misuse?

Yes	26%

Q. Does your organization have written rules governing personal e-mail use?

Yes	68%

EXECUTIVE SUMMARY: INSTANT MESSAGING RISKS & RULES, POLICIES & PROCEDURES

While 35% of employees use IM at work, only 31% of organizations have IM policy in place, and only 13% retain IM business records. With 50% of workplace users downloading free IM tools from the Internet—a dangerous practice that 26% of employers aren't even aware of—the lack of written IM rules opens organizations to tremendous risk. Employees' use of public IM tools coupled with ill-advised content including attachments (26%); jokes, gossip, rumors, and disparaging remarks (24%); confidential company, employee, and client information (12%); and sexual, romantic, and pornographic chat (10%)—make workplace IM a recipe for legal, regulatory, and security disaster.

FINDINGS: WORKPLACE IM

Q. Do you use instant messaging (IM) at work?

Yes	35%

Q. If yes, what type of IM tool do you use?

Free IM software downloaded from Internet	50%
Employer-provided IM system	50%

Q. If you are using a free IM tool that you downloaded, is your employer aware?

Yes	47%

Q. Does your organization have a written policy governing IM use and content?

Yes	31%

Q. Have you ever sent or received an instant message at work that contained any of the following content?

Sexual, romantic or pornographic content	10%
Jokes, gossip, rumors or disparaging remarks	24%
Confidential information about the company, a co-worker, or yourself	12%
Attachment of any kind	26%

Q. Has your organization ever been ordered by a court or regulatory body to produce employee IM? (In other words, has employee IM ever been subpoenaed?)

Yes	1%

Q. Has your organization ever fired an employee for IM misuse?

Yes	2%

EXECUTIVE SUMMARY:
BLOG RISKS & RULES, POLICIES & PROCEDURES

When it comes to potential risks, unmanaged blogging dwarfs e-mail and IM. Among the blog risks detailed by ePolicy Institute Executive Director Nancy Flynn in her new book *Blog Rules* (AMACOM, July 2006) are copyright infringement, invasion of privacy, defamation, sexual harassment and other legal claims; trade secret theft, financial disclosures, and other security breaches; blog mob attacks and other PR nightmares; productivity drains; and mismanagement of electronic business records.

According to the survey, 8% of organizations operate business blogs. In spite of the risks, only 9% have policy governing the operation of personal blogs on company time; 7% have policy governing employees' business blog use and content; 7% have rules governing the content employees may post on their personal home-based blogs; 6% use policy to control personal postings on corporate blogs; 5% have anti-blog policies banning blog use on company time; and 3% have blog record retention policies in place.

With 55% of business blogs "facing out," for customers and other third-parties to read, the lack of written blog rules is a potentially costly oversight. Considering that less than 2% of organizations assign a lawyer or other responsible party to review employees' entries and third-parties' comments prior to posting, the enforcement of written usage and content rules is a business-critical best practice for any organization engaged in blogging.

In addition to policy, employers are taking advantage of technology tools to help manage employees' blog use (and misuse). In fact, 17% of companies use technology to block employee access to external blog URLs, and another 12% regularly monitor the blogosphere to see what is being written about them. As revealed by the 2005 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute, blog monitoring and blocking lags behind Internet and e-mail surveillance. Fully 76% of employers monitor employees' Website connections; 65% use technology to block connections to banned Websites; and 55% monitor e-mail.

Employee bloggers, who can be fired, or "dooced" in blog parlance, for blogging at work (and at home on their own computers) face increasing risk of termination by employers struggling to keep a lid on legal claims, regulatory fines, and security breaches. With the blogosphere growing at the rate of one new blog per second, industry experts expect the ranks of dooced employee bloggers to swell.

As detailed in *Blog Rules*, employee bloggers mistakenly believe the First Amendment gives them the right to say whatever they want on their personal blogs. In fact, the First Amendment only restricts government control of speech; it does not protect jobs. Bloggers who work for private employers in employment-at-will states can be fired for just about any reason—including blogging at home on their own time or at the office during work hours. In spite of the confusion, fewer than 2% of organizations have educated employee-bloggers about the First Amendment and privacy rights.

FINDINGS: BUSINESS BLOGGING

Q. Does your organization operate a business blog?

Yes	8%

Q. If yes, what type of business blog is it? (Check all that apply)

External or "facing out" blog for customers and other third-party readers	55%
Internal blog for employees only	48%
CEO blog	16%

Q. What type of written blog rules and policies does your organization have in place? (Check all that apply):

Policy governing employees' business blog use and content	7%
Rules governing the content employees may post on their personal, home-based blogs	7%
Policy governing personal postings on corporate blogs	6%
Policy governing operation of personal blogs on company time	9%
Anti-blog policy banning blog use on company time	5%
Policy governing the retention of blog business records	3%

Q. Does your organization regularly monitor the blogosphere to see what is being written about it?

Yes 12%

Q. Does your organization use technology to block access to external blog URLs?

Yes 17%

Q. Has your organization ever fired an employee for misusing the corporate blog?

Yes 0.3%

Q. Has your organization ever fired an employee for content posted on the employee's personal, home-based blog?

Yes 1%

Q. Has your organization educated employee bloggers about the First Amendment and privacy rights?

Yes 2%

Q. Does your organization post comments from customers and other outsiders on its corporate blog?

Yes 3%

Q. Does your organization assign a lawyer or other responsible party to review blog content prior to its being posted?

Review employees' entries prior to posting? 1%

Review third-party comments prior to posting? 1%

Q. Has your organization ever been attacked by an organized blog mob?

Yes 1%

Q. Has your corporate blog triggered a legal claim (copyright infringement, invasion of privacy, sexual harassment, trade secret theft, hostile work environment, etc.?

Yes 0.3%

EXECUTIVE SUMMARY:
ELECTRONIC BUSINESS RECORD RISKS & RULES, POLICIES & PROCEDURES

Employers eager to minimize electronic risks and maximize employee compliance should start with written rules, including policies governing the retention of electronic business records—the electronic equivalent of DNA evidence.

Overall, employers are not doing an effective job of managing electronic business records, the evidence that can make (or break) a company's legal position. Merely 34% of companies have written e-mail retention/deletion policies in place, in spite of the fact that 34% of employees don't know the difference between business-critical e-mail that must be saved and insignificant messages that may be purged. Even fewer organizations have policy in place to manage the retention and archiving of IM (13%) and blog (3%) business records.

FINDINGS: ELECTRONIC BUSINESS RECORDS

Q. Do you know the difference between an electronic business record (e-mail, Instant Message) and an insignificant message that is not a record?

Yes 57%

Q. Has your organization provided employees with a formal definition of "electronic business record"?

Yes 21%

Q. Does your organization have a written e-mail retention and deletion policy and schedule in place?

Yes 34%

Q. Does your organization retain and archive IM business records?

Yes 13%

Q. Does your organization have a policy governing the retention of blog business records?

Yes 3%

Respondent Profile

Number of survey respondents	416
Number of employees per company	
100 or fewer	35%
101–500	19%
501–1000	7%
1001–2500	11%
2501–5000	8%
More than 5000	20%

Industry

Business/Professional Services	22%
Financial Services	13%
General Services—For Profit	3%
General Services—Nonprofit	5%
Manufacturing	15%
Public Administration	6%
Wholesale/Retail	4%
Other	32%

The **2006 Workplace E-Mail, Instant Messaging & Blog Survey** is co-sponsored by American Management Association (www.amanet.org) and The ePolicy Institute (www.epolicyinstitute.com). A total of 416 companies participated: 35% represent companies employing 100 or fewer workers, 101–500 employees (19%), 501–1,000 (7%), 1,001–2,500 (11%), 2,501–5,000 (8%) and 5,001 or more (20%). In 2005, 526 U.S. businesses participated in the Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute. In 2004, 840 U.S. businesses participated in the 2004 Workplace E-Mail and IM Survey from American Management Association and The ePolicy Institute. In 2001, 435 organizations participated in the 2001 Electronic Policies and Procedures Survey from American Management Association and The ePolicy Institute.

The **2006 E-Mail, Instant Messaging & Blog Survey** questionnaire was designed by American Management Association and The ePolicy Institute's Nancy Flynn, author of ***Blog Rules*** (AMACOM 2006), ***Instant Messaging Rules*** (AMACOM 2004), ***E-Mail Rules*** (AMACOM 2003), and ***The ePolicy Handbook*** (AMACOM 2001). Comparative numbers drawn from the **2004 Workplace E-Mail & Instant Messaging Survey** from American Management Association and The ePolicy Institute; and the **2005 Electronic**

Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute.

Media wishing to receive a review copy of **BLOG RULES:** ***A Business Guide to Managing Policy, Public Relations, and Legal Issues*** by Nancy Flynn (Amacom, July 2006), should contact AMACOM's Irene Majuk (212-903-8087 or imajuk@amanet.org). Contact AMA's Roger Kelleher (212-903-7976 or rkelleher@amanet.org) for survey process. Contact the ePolicy Institute's Nancy Flynn (614-451-3200 or nancy@epolicyinstitute.com) for interviews and information about workplace e-mail, IM & blog risks, policy and best practices.