

The biggest e-mail blunders of 2003

Tips on avoiding e-mail gaffes in the coming year

Corporate e-mail gaffes triggered costly disasters in 2003, from high-profile lawsuits and million-dollar regulatory fines to humiliating public revelations about employees' private lives.

In hopes that last year's expensive e-mail gaffes will serve as a wake-up call for business, The ePolicy Institute, a source of e-policy, e-mail and instant messaging-related services and products, and Clearswift, a provider of software for managing and securing electronic communications, have identified the biggest e-mail blunders of 2003, featuring the year's top five e-mail mistakes and tips for avoiding similar disasters in 2004.

According to Nancy Flynn, executive director of The ePolicy Institute and author of "E-Mail Rules," the blunders of 2003 underscore the need for organizations to establish e-mail policies, educate employees about e-mail risks and rules and enforce e-mail policy with software.

No. 1. — Failing to keep content clean, compliant, and corporate: Enron employees learned a hard lesson about keeping personal and business e-mail separate.

Because Enron employees regularly used the company's e-mail system for personal communication, private messages were retained alongside Enron's electronic business records. Consequently, employees' personal e-mail was collected as evidence during the Federal Energy Regulatory Commission (FERC) investigation of Enron's alleged energy-market manipulation.

When in 2003 FERC posted 1.6 million Enron e-mails online, employees' private correspondence went on public display. Employee romances, affairs, and marriages were discussed, executive salary packages and employee performance reviews were transmitted, employees' bank records and Social Security numbers were displayed—all with senders' and receivers' names attached.

FERC eventually removed e-mails containing Social Security numbers and employee performance evaluations, but not before the Enron e-mail disaster was covered by the national business media, and millions of curious readers (including identity thieves and other malicious outsiders) jumped online to sort through the goldmine of Social Security numbers, personal dirt, and other "goodies."

A cautionary tale for all corporate e-mail users, the Enron e-mail disaster



Investment banker Frank Quattrone discovered it's illegal to destroy e-mail evidence.

drives home an important lesson for employees. Never use your employer's e-mail system to transmit personal, sensitive or confidential information that would embarrass you or harm your loved ones were it made public.

For employers, the Enron e-mail disaster clearly illustrates why it is so important to distinguish business record e-mail from inconsequential messages, and to purge all e-mail that need not be retained for business, legal, or regulatory purposes.

No. 2. — Failing to retain business record e-mail: Investment banker Frank Quattrone discovers it's illegal to destroy e-mail evidence.

Quattrone was accused in 2003 of obstructing federal grand jury and Security and Exchange Commission investigations after he forwarded an e-mail urging members of his technology sector banking group at Credit Suisse First Boston (CSFB) to "clean up" their files.

At the time he sent the e-mail, the grand jury and regulators were investigating whether CSFB accepted kickbacks from hedge funds in exchange for hot IPOs. The file cleanup missive was just one of several e-mails that prosecutors used as evidence in the high-profile, widely publicized case against Quattrone.

The case, which ended in a mistrial, gives individual e-mail users a new rea-

son for concern. Under the legal principle of vicarious liability, employers are typically held responsible for the wrongful acts of employees. In the Quattrone case, however, the individual, not CSFB, was held responsible for ordering the deletion of e-mail files.

Quattrone's trial illustrates why corporate e-mail users should strictly adhere to the organization's e-mail retention strategy, and never destroy e-mail evidence after an inquiry begins. Employers have been slow to learn this lesson despite growing scrutiny from courts and regulators.

According to the 2003 E-Mail Rules, Policies, and Practices Survey from American Management Association (AMA), The ePolicy Institute, and Clearswift, only 34 percent of employers have written e-mail retention and deletion policies in place. That's the same figure reported in 2001, a year before five Wall Street brokerage firms were fined \$8.25 million by the SEC for failing to retain e-mail in accordance with regulations.

No. 3. Failing to educate employees: Merrill Lynch experiences the sting of negative e-mail-related publicity.

Ask yourself: How would I feel if this message appeared on the front page of a newspaper? Two senior executives of Merrill Lynch experienced the sting of negative publicity firsthand when an e-mail message in which they cautioned 50,000 employees to be mindful of e-mail content was covered by the national business media.

Don't leave employee education to chance. Cover content, confidentiality and compliance concerns in your e-mail training program. You never know when a disgruntled employee or vengeful former employee will share a confidential internal e-mail message with the media, competitors, or other outsiders.

Unfortunately, only 48 percent of organizations offer e-policy education to employees, and merely 27 percent train staff about e-mail retention rules, according to the 2003 E-Mail Rules, Policies, and Practices Survey from AMA, The ePolicy Institute, and Clearswift.

E-mail training is central to sound e-risk management. Not only is an educated work force more likely to comply with written e-mail rules, but the courts and regulators tend to respond favorably to policy and training consistently applied. The U.S. Supreme Court has

made it clear that through the development and enforcement (including employee training) of comprehensive e-mail policies, an organization may be able to create a defense against sexual harassment or hostile work environment liabilities stemming from employee e-mail.

No. 4. — Failing to monitor employees' e-mail use: Big Brother watches as American Family Insurance employee wilts.

A 2003 undercover investigation of the Yahoo! "Candyman" e-group led the FBI to suspect that an employee of American Family Insurance was using the company's e-mail system to receive child pornography.

When the employee tried to suppress evidence found during the FBI's search of his work computer, the court ruled that he had no expectation of privacy, given his employer's computer-related rules, policies, and procedures.

American Family Insurance had a log-in notice that warned of possible monitoring or searching, and required users to click "OK" to proceed. Every time the defendant accessed his work computer, he consented to his employer searching his computer. The company also posted e-policies on its intranet site and sent e-mail notices to employees reminding them of the policies.

The court stated: "An employee cannot claim a justified expectation of privacy in computer files where the employer owns the computer; the employee uses that computer to obtain access to the Internet and e-mail through the employer's network; the employee was explicitly cautioned that information flowing through or stored on computers within the network cannot be considered confidential; and where computer users were notified that network administrators and others were free to view data downloaded from the Internet."

Savvy employers are catching on to the wisdom of monitoring external e-mail communications. According to the 2003 E-Mail Rules, Policies, and Practices Survey from AMA, The ePolicy Institute, and Clearswift, 51 percent of employers monitor incoming e-mail, and 39 percent keep an eye on outgoing e-mail. Where employers fail to focus, however, is with the internal e-mail communications that take place among employees. Only 19 percent of organizations monitor internal employee e-mail.

"Management's failure to monitor internal e-mail discussions among

employees is a potentially costly oversight," says Greg Hampton, vice president at Clearswift. "E-mail messages between employees are exactly the type of casual, off-the-cuff communications that tend to contain inappropriate, offensive content that may trigger claims of a hostile work environment, sexual harassment, or racial discrimination."

Don't leave e-risk management to chance. Keep online employees in-line by: 1) Establishing written e-mail rules and policies; 2) Educating all employees, from entry-level staff to the CEO; and 3) Installing policy-based content filtering software.

No. 5. — Failing to recognize — and manage — instant messaging as a high-risk business tool. Instant messaging is used in 90 percent of offices — without management's knowledge or authorization.

Instant messaging is a form of turbo-charged e-mail that creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations.

An internal survey revealed that more than half of the 1,300 employees of regional stock brokerage firm Stifel Nicolas had downloaded free instant messaging software from the Web, without management's knowledge or approval. Brokers were using instant messaging without the authorization of the firm's compliance department, which is charged with ensuring that the firm adheres to recently tightened SEC, NASD, and NYSE regulations covering the management, monitoring, and retention of instant messages.

The government and industry regulators who oversee financial services firms are serious about instant messaging and e-mail compliance. Five Wall Street brokerages were fined \$8.25 million for violating SEC e-mail retention rules in 2002. Securities firms that violate regulators' instant-messaging rules, intentionally or accidentally, should expect to be hit with equally robust penalties.

Stifel Nicolas is not alone. It's estimated that instant messaging is used in 90 percent of offices. In many cases, employees have downloaded free software from the Web and are instant messaging clients, competitors, and colleagues without management's knowledge, written rules and policies to guide usage, or IT-approved technology to help prevent security breaches and control overall risk.

Regulated or not, it is imperative for organizations large and small to take control of instant-messaging risks today, or face potentially costly consequences tomorrow.

As detailed in Nancy Flynn's forthcoming book, "Instant Messaging Rules," employers who mistakenly view instant messaging as "emerging" technology can

no longer afford to remain in the dark about employees' instant messaging use. Organizations must act now to uncover and control the practice. Fail to manage it today, and you'll likely face potentially costly risks on the security, privacy, legal, regulatory, productivity, compliance, and technology fronts tomorrow.

Don't wait for a high-profile, potentially costly e-disaster to strike your organization. Take action now by developing and implementing e-mail and

instant-messaging rules and policies that clearly detail how your employees may (and may not) use your computer system. Back up written policy with comprehensive employee education to ensure that senior executives and staff understand e-mail and instant-messaging risks, and recognize the importance of complying with e-policy. Finally, enforce your policy and training program with policy-based content filtering software that works in concert with your written e-

mail and instant-messaging policies.

According to The ePolicy Institute and Clearswift, employers cannot afford to treat e-mail and instant messaging as convenient communications tools like the telephone. The electronic equivalent of DNA evidence, e-mail and instant messages produce written business records that must be managed, monitored, retained and archived.

For more information: www.epolicyinstitute.com **T**



the moment of proof

on television in print online on radio

We don't just deliver results. We exceed expectations.

The project went live and you delivered incredible broadcast results. You partnered with professionals who provided expert consulting and powerful distribution to news media. You had the best television placement, tracking and monitoring and could guarantee radio listeners and Internet users.

Success is a foregone conclusion when you rely on proven leaders.

Headquarters in NY with offices in major US cities and an international hub in London

MediaLink

800 843 0677 212 682 8300 info@medialink.com www.medialink.com

Copyright of Public Relations Tactics is the property of Public Relations Society of America and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.