



Watch What You Say!

Everyone has heard the stories about law suits won against a company because of an email an employee sent. Chevron paid \$2.2 million in damages to a group of women employees that filed suit when a joke entitled "25 reasons beer is better than women" was widely distributed throughout the company via email. In *Betts v. United Airlines* the claim was that disparaging comments were made regarding an employee to other employees via email and that the company should be held liable. The court agreed.

Employees do not, in most cases, intend to cause harm to their company but are often unaware of how a seemingly innocent email can have disastrous consequences. A company has responsibility to take steps to ensure all email is business appropriate.

Steps to Take to Reduce Liability

- 1. Write an email policy.** The policy should clearly state what comprises appropriate and inappropriate use of company email. The policy should state the specific consequences if the policy is violated. It should also cover the company's email monitoring policy and specifically state that emails are not private. The written policy should be given to every employee. It is good practice to have the employee sign acknowledging receipt of the policy as well as when updates are distributed.
- 2. Train employees on appropriate email content.** This should be part of every company new hire program and should include training on appropriate email content. Retraining annually will keep the awareness in the forefront of every employee's mind as they go about their everyday jobs. (ISC's *Think Before You Click*®--a short eLearning email awareness course is available at a price point every organization can afford). Training should cover the company email policy and include specific examples of seemingly innocent email content that could be considered inappropriate and harmful.
- 3. Enforce email policy.** Prompt action should be taken by the employer when any complaints are registered and, if appropriate, the disciplinary action outlined in the email policy should be applied.
- 4. Monitor employee communications.** It is good business sense for organizations to monitor their email communications. History has shown that companies have been held liable even when management was not aware of the inappropriate email activities. Large organizations utilize email monitoring software that search for patterns, words and user-defined criteria. Smaller organizations may include monitoring as part of the job of a human resource professional.

5. **Notify employees that email is monitored.** A powerful behavior modification tool is notifying employees that on a specific date email correspondence were monitored in accordance with the company email policy. This makes the email policy real to every individual in the company. A goal to monitor every employees' email correspondence once each year will send the message that the company is serious about enforcing the email policy.
6. **Add a disclaimer.** Consider adding a disclaimer to all email signatures that the electronic communication is not intended to constitute an offer or acceptance of any agreement to avoid being misconstrued as an electronic signature for contractual purposes. The company legal department should prepare the disclaimer.

The Bottom Line

When all the appropriate steps are taken to reduce email risks there are some unintended benefits. With the non-conforming email disappearing from the company landscape after implementing the steps above, IT departments notice that network traffic is reduced, bandwidth requirements lessen, and server capacity increases. Creating, monitoring, and enforcing an email policy is a smart business practice.