Email Forensics Expert:
Managing the Risky Business of Company E-mail

Part 1 of 2

By Scott Greene

Digital Evidence / Computer Forensics Articles

As an employer, Human Resources Director, or Risk Management Supervisor, ask yourself this question: "Do our employees think about the legal risk of sending communications over the internet?" If you are like the majority of companies, your answer would be, "It is highly improbable". It is a very common problem amid the work place, for an employee to believe their electronic communications are transient, temporary and, once deleted, untraceable and therefore, harmless.

The fact is e-mail, faxes and even cellular phones leave a trace. Just one e-mail sent from your employee to the employee of a different company passes through an average of four different computer systems. This creates a trail making e-mail real, traceable, and permanent.

As an industry leader in Computer and Technology Forensics for the past 20 plus years, we have documented, during the examination of electronic systems, employees who frequently say/save things into e-mails or store on a computer, things they would never say anywhere else. Either having an employee delete a potentially damaging or inflammatory e-mail or even an employee deleting an e-mail on their own, does not protect anyone. In fact, it could in the end harm everyone involved.

If a complaint or inappropriate conduct of an employee has risen to the level where you as an owner/supervisor, need to consult a Computer and Technology Forensics expert, one of the first areas checked is for deleted documents and/or e-mails. These items cause red flags during an examination of equipment, and the original items can and most likely will be found and/or reconstructed. It is very important to understand that the intentional destruction of evidence is a felony, and if proven, could land one in jail.

An example of computer message in a court case dates back to the infamous trial of some of the Los Angeles Police being tried in the 1991 beating of Rodney King. One of the officers created a computer message stating, "…….I haven't beaten anyone that bad in a long time." This obviously became admissible in court.

A more recent example, is one in which we as a company were hired in a libel case. The libeler was using the internet to post messages on a public bulletin board that were both slanderous and libelous against a competitor in the same field. This person felt that by using "anonymous" e-mails and postings, this would increase their own standing within the same professional community. What the libeler didn't count on was the traceability of the e-mails to their home, cell phone and company computer systems. We were able to locate the electronic trail, and with this information obtain, on behalf of the client, a court order to confiscate the equipment in order to create image copies of the electronic systems. As a result, in order to keep the issue private, the libeler agreed to a significant out of court settlement.

Part Two: How To Manage the Risky Business of Company E-mail.

Author's note: The suggestions listed in this article are not meant to be all inclusive and are not legal advice. It is based upon our 30 plus years of experience in the industry as professional Computer and Technology Forensics experts, and how you, as an owner/supervisor, can potentially avoid legal pitfalls.

Scott Greene is the founder and CEO of Evidence Solutions, Inc. which has been an industry leader in Computer Consulting and Technology Forensics since 1982.

Call us today with your Digital Evidence Questions: 866-795-7166 or Sales@EvidenceSolutions.com

Related Articles:
Trends in Technology 2014
Who is Watching You Online?
Law Firms Must Step Up Cybersecurity!
Email System Forensics
Sample Computer and Email Usage Policy.
Employee Theft of Intellectual Property

Complex Electronic Evidence in PLAIN English.

Like Evidence Solutions - Electronic Evidence on Facebook

Follow Evidence Solutions - Digital Evidence Division on LinkedIn

Circle Evidence Solutions - Digital Evidence Division on Google+

Google+ Author

Google+ Publisher