HOW TO REDUCE THE LEGAL RISKS OF EMESSAGING

BY STEVE MACKES

You'd think by now, given what happened some years back with Enron and Microsoft and a host of other companies, most everyone would know. But based on what continues to pop up in the news—think Tiger Woods, Ohio State Football Coach, Jim Tressel and financial institutions like Goldman Sachs—it's clear that many still have not received the memo, which is E-MESSAGES CAN INCRIMINATE!

It makes one wonder why, in this world of increased litigation, investigations and compliance mandates, otherwise savvy and careful individuals and businesses continue to underestimate the risk inherent in e-messaging. The answer appears to lie with the very nature of this kind of electronic communication.

Whether it involves emails, texting, or posting on social media sites like Facebook and Twitter, e-messaging feels informal, which, in many instances, causes people to let down their guard and say things they might, otherwise, not say. Further feeding that casual mindset is that e-messaging is often quickly received and responded to in an impulsive and emotional way, its immediacy trumping the urge to stop and reflect for a few moments on what someone might actually be saying. Also, because these messages lack that hard copy, hold-in-your-hand feel of permanence and are sent out into the ether, across the Internet, they seem like a kind of transient, anonymous, free-form interaction that is fleeting and without consequence.

In actuality, however, these are all misconceptions that couldn't be further from the truth and only add to the risk and potential liability inherent in electronic communications. For your own awareness and protection, here are some sobering facts—what every individual and business should know—about e-messaging:

- E-messages are pretty much permanent. A deleted message resides on a computer or network until it runs out of free space, whereupon deleted files begin to be overwritten. Until then, deleted files can be retrieved by computer experts. Every e-message is being recorded somewhere—on a company's network server, by an Internet or mobile service provider, on a computer hard drive or within Cloud storage.
- Electronic messaging in all of its forms are, more and more, used as evidence in litigation.

- Companies are required by law to retain email messages for a minimum of 2 years. Electronic attachments to messages provide much more information than what is seen on the screen. Every attachment contains metadata, which is essentially embedded background information about the content, quality, condition and other characteristics of data. Through metadata, virtually every keystroke, every typo, every trace of a document's different incarnations can be traced.
- Non-company-related emails, generated at work, do not belong to the person who created them. Any emails generated at work, regardless of their nature, immediately become the property of the person's employer.
- Emails are considered privileged information and off-limits to investigators only when they are lawyer-client communications.
- If an email sent to 5 people becomes potential litigation evidence, the number of files that will have to be examined can easily grow exponentially to include not only all of the files those 5 received but also the files of anyone who might have had the email in question forwarded to them.

It's not just business executives and corporations who fall into the e-message trap. Recently, celebs such as Kanye West, Chris Brown and George Lopez have been called out for their e-messaging and then compelled to backtrack or apologize. As bad as those incidents might seem, they're minor compared to some examples of e-message mismanagement.

Frank Quattrone, former head of Credit Suisse First Boston was convicted of obstructing justice and faced 25 years of imprisonment. His crime was sending emails encouraging the destruction of files while there was an ongoing criminal investigation of CSFB. One such email, titled, "Time to clean up files" was sent 2 days after Quattrone learned of the investigation by the Justice Department.

In Microsoft's anti-trust case, email played an important role in exposing the real intentions of Bill Gates and his company to undermine competitors such as Real Networks, Sun Microsystems and, in particular Netscape. One Microsoft email asks: "How much do we have to pay you to screw Netscape?" While another, written by Microsoft VP Paul Maritz describes the plan to crush competition from Netscape. He says: "We are going to cut off their air supply. Everything they are selling, we are going to give away for free." Even though this case was eventually settled, Microsoft was compelled to pay some 4.5 billion dollars to infringed parties, largely because of incriminating messages like those mentioned above.

But being used as evidence in litigation isn't the only threat posed by e-messages. There's also the possibility that sensitive product or other information can be stolen. The Gillette Company found this out the hard way when they discovered that a contract employee was using email to steal and then sell plans for the company's new Mach-3 razor.

E-message Guidelines

When it comes to e-messaging, there are 4 simple guidelines to follow that can potentially keep you and/or your company out of harm's way.

Watch what you say.

Though e-messages can be scrutinized by management at any time and easily distributed to the world, employees remain amazingly laid-back and complacent about what they say in them. As a good rule of thumb, do not put anything into an e-message that you would not be prepared to say out loud. In front of your mother. In Court. Do not write anything that you would not want to be tomorrow's Wall Street Journal headline.

Understand that electronic documents pretty much last forever.

When documents are deleted, there is still a record on a hard drive, and it is retrievable until it is written over. Given the capacity of today's computers, with hard drives of hundreds and thousands of gigabytes, it is doubtful that e-messages are ever written over. And if not, persons skilled in forensic retrieval can get at that information.

Distribute e-messages only to those who need the information.

The more you can effectively limit the spread of e-messages, the better. Rather than automatically hitting the 'Reply to All' button, carefully consider to whom you are distributing information. Suppose an email is sent to 7 persons, and 3 of the recipients forward the email to 5 additional people. In discovery, lawyers will be obligated to search the files of all persons who wrote or received the email, in this instance 12 persons. It's easy to see how a case could require thousands of documents and numerous hard drives to be reviewed, dramatically increasing both potential liability and legal expense.

Be careful about the language you use in e-messages.

Never write e-messages when your emotions are raging. Anger and sarcasm often come across stronger in text than they would in person. Also, think about your choice of words, and don't use all caps because it looks like you're SHOUTING. Punitive words like 'punish,' or 'teach a lesson' can seem to indicate a state of mind to harm and, at the very least, reflect poorly on the sender. You should also be very careful about making any references to age, race or gender. One more thing to watch out for is inappropriate humor. Don't send potentially offensive email such as jokes, questionable images, etc. When uncertain if something crosses the line, err on the side of caution.

Following these simple guidelines can help keep your emotions and potential liability in check when sending e-messages. That, in turn, can go a long way toward keeping you out of the news, out of court, out of jail and generally, out of trouble.

How GRM Document Management Helps

Barcode, complete chain-of-custody tracking. Document Retention—getting rid of information no longer needed. EDM allows prompt response to information requests. Everything is organized and easily located; no lost or misplaced documents. Security of the systems and facilities to prevent problems such as identity theft, information hacking and corporate espionage. Scanning and imaging services as well as digital web hosting allows physical information to be converted and distributed quickly.

More About GRM

GRM Document Management is a leading provider of lifecycle records and information management solutions. The company brings proprietary innovation, blended integration and new levels of cost efficiency to document storage, data protection, digital/electronic document management and certified destruction. With over 24 years of experience, GRM has earned the trust and continued business of more than 5,000 customers—large and small, domestic and multinational—representing a wide range of industries. Clients are served from state-of-the-art, climate-controlled facilities in major U.S. markets and internationally throughout China.