Everlasting Evidence: E-Mails Are Forever

9/4/2012 By Bill Leonard

E-mails are forever.

No, that isn't the title of the latest James Bond thriller but a message that many attorneys and corporate security experts have been trying to tell business leaders for years. While some have listened, many still haven't heeded the warnings.

"E-mails are the everlasting evidence," said Mindy Chapman, an attorney and president of New York consulting group Mindy Chapman and Associates. "Just because you hit delete doesn't mean that e-mail is gone for good. There are backup files and servers that e-mails will stay on forever."

Electronic evidence discovery has become an integral part of the process of preparing legal cases—for plaintiffs and for defendants. E-mails and other information placed on the Internet, intranets and local servers aren't easily destroyed or shredded like hard-copy records. Electronic files are typically stored on backup servers and, even if deleted from a server or computer hard drive, leave residual traces that computer forensic specialists can recover.

"I always tell clients that if you have some issue or situation that is best shared by talking it through with someone, then pick up the phone and give that person a call or walk down the hall and talk to them in person," Chapman said. "Because once you put it into an e-mail, then that message is going to last forever."

An Essential Work Tool

As scary as that might sound, e-mails and electronic communications have become essential to working and conducting business, and most organizations do have e-mail, electronic device and Internet usage policies in place. The problem is many people don't follow these policies, and this can create huge headaches for businesses and their human resource departments because protecting the integrity of an organization and avoiding legal entanglements becomes virtually impossible.

E-mail policies and protocols differ among organizations, often varying depending on the industry. For example, the financial industry is highly regulated, and information shared electronically both internally and externally is examined carefully by government agencies. Still, any e-mail and Internet usage policy should include specifics on what constitute proper and improper messages. In addition, the policy needs to address sharing private information about employees and protecting the organization's proprietary data.

"Somewhere along the line, HR has become something of the de facto compliance officers for many organizations," said Aaron Titus, chief privacy officer for Identity Finder in New York City. "And that means it often falls on the shoulders of the HR department to make sure everyone in the organization understands and follows e-mail and Internet usage policies."

A Common Thread

Stories about organizations or executives ensnared in controversy and possible wrongdoing are commonplace these days. A common thread is that the evidence of improper sharing or use of information was uncovered through e-mails.

Most employers have policies in place to keep employees from improperly sharing sensitive information and sending messages that reflect badly on the organization. While some people might forward jokes or photos they find amusing, these messages can be construed differently by others. Claims of discrimination, sexual harassment and hostile work environment have been built on this type of e-mail evidence. In addition, improper sharing via e-mails of sensitive employee information such as compensation and health benefits have created problems for employers, so there are legitimate business and legal compliance reasons for electronic usage policies.

Two recent stories that made worldwide headlines show just how damning e-mail evidence can be. In one story, it was revealed that high-ranking officials at Penn State University had e-mail discussions about how to deal with allegations that an assistant football coach was sexually abusing young boys who attended a university-sanctioned football camp. In the other story, e-mail evidence showed that top-level executives and board directors at several leading banks in the United Kingdom conspired to release false and misleading reports on the banks' lending rate costs known as the London Interbank Offered Rates, or LIBOR. In the LIBOR case, international lending institutions such as Barclay's Bank allegedly manipulated the lending rates and then profited from the false reports—much of which was communicated through e-mails.

In both cases, top officials lost their jobs when the evidence came to light.

While sources for this article said those two cases are extreme examples, dozens of employment-related lawsuits have hinged on e-mails that defendants claim were taken out of context, according to Jonathan Yarbrough, a partner in the Asheville, N.C., law office of Constangy Brooks and Smith, LLP.

"Once in a while, you might find the 'smoking gun' evidence in an e-mail, but often e-mail evidence is only part of the puzzle when building a case," Yarbrough said. "E-mails can be evidence of patterns and behaviors, like improper sharing of private and proprietary information. And often e-mails at first glance may not seem to be relevant and appear innocuous, but these same e-mails can still indicate and establish a pattern of behavior."

“There will always be bad actors and people who are deliberately doing the wrong thing. Thankfully, e-mail evidence can help to catch and stop them,” Titus said. “However, the vast majority of employers are really trying to do the right thing and abide by the law, but then they get caught in bad situations because someone didn’t follow proper e-mail protocols.”

The Wrong Attitude

With dozens of cases in which e-mail evidence has come back to haunt organizations and their executives, why does it keep happening?

“I think the attitude many people have when they read or hear about these stories is ‘Oh, that just doesn’t apply to me or this organization,’ ” Titus said. “And that’s a pretty risky attitude to take.”

According to Titus, the best thing an employer can do to ensure that its e-mail and Internet usage policies are followed is to get full buy-in from every person in the organization.

“What I mean by buy-in is that everyone understands and agrees to abide by the organization’s policies fully,” he said. “They also need to be completely aware of the consequences of not following the policy and how it will directly affect them. Once they really and truly understand that, then they will know just how important these policies are to ensure the security of the organization and to protecting their privacy.”

The Value of Training

HR departments have an important role to play in communicating, training, and then making sure everyone understands and adheres to the policy, according to Chapman. She doesn’t particularly like the term buy-in because she believes agreeing to work at an organization should be a commitment to adhere to all company employment policies and conditions.

“When someone comes to work at your organization, they’ve already bought into the conditions of employment. What employers must do is properly train employees about these policies and communicate exactly how they work,” Chapman said. “I will routinely ask clients if they have an anti-theft policy and what they do if an employee breaks that policy. I then will ask them ‘So, tell me how is it different when an employee breaks the rules of the organization’s e-mail policy?’ ”

Chapman recommends vigorous training and communication of corporate electronic messaging and Internet usage policies. Employees at all levels must understand what the policies mean and the importance of following them.

“Employers should incorporate something in their employee orientation about e-mail etiquette, and then they should follow it up once a year as an addendum to any kind of annualized training program that they do,” said Steve Hyatt, vice president of human resources for the east region of Gannett Co. Inc. “As an HR generalist with 30 years of experience, I can’t tell you how many times I’ve seen people get in the middle of a confrontation because of inappropriate e-mails they sent out that were based on an emotional explosion and then they’re embarrassed later by it.”

A Tough Challenge

An emotional response shared via an improper e-mail can prove more embarrassing and public if it comes from someone high up in the organization.

The easy part for HR appears to be getting most employees from mid-level managers down to entry-level employees to understand and follow corporate e-mail policies. The tougher challenge, experts say, is making sure that upper-level managers and board directors do the same.

“One of the top questions HR practitioners ask me is ‘How can we get upper-level management on board with this?’ ” said Yarbrough, who has led seminars and training sessions on corporate Internet usage policies. “And the answer often depends on if the organization’s HR department has a seat at the table and is respected by upper-level management. Sometimes, sadly, that’s just not the case and that actually becomes a much bigger issue for HR to address.”

Still, HR has a crucial role to play in ensuring that e-mail and other organizational policies are followed by employees at all levels. In fact, an independent investigation of the situation at Penn State found that the university’s HR department had been kept out of the loop and therefore did not have the opportunity or authority to investigate the allegations properly. Former FBI Director Louis Freeh conducted the investigation and recommended **in his written report** that Penn State officials needed to “assign all HR policy-making responsibilities to the office of human resources and limit the ability of individual departments and campuses to disregard the university’s HR policies and rules.”

Getting Senior Management On Board

Unfortunately, disregarding rules and policies is common among upper-level managers at many organizations. Both Yarbrough and Chapman agree it is a serious problem that often has serious repercussions for businesses.

“Corporate policies must apply to everyone in the organization—no exceptions,” Chapman said. “Some senior-level executives might not believe this is true, and what I typically ask when I hear this is ‘So the rules don’t apply to you, and that’s going to be your defense when a lawsuit or criminal charge is filed? Just how do you think that’s going to fly when you tell this to a judge and jury?’ ”

Chapman is adamant that upper-level executives and board directors must be trained to follow corporate e-mail and Internet usage policies just like anyone else in the organization. “They tend to be the face and voice of the organization, and therefore they need this type of training the most,” she said.

“It’s the only way that the policy will work and be effective throughout the organization,” she said. “Many upper-level executives understand this and set good examples for their organizations, and that’s the way it should be.”

Finding Allies

However, this isn’t always the case, and HR often doesn’t have the authority or clout to ensure adherence by C-suite executives.

Yarbrough and Titus recommend that HR directors and managers look for allies in the organization who can make sure the message is heard in the C-suite. Corporate in-house counsels, chief information officers and chief financial officers often have the ear of the CEO and the board and can be effective partners for HR.

“Chief information officers understand the systems and the problems errant e-mails can create, and a CFO can certainly understand the bottom-line impact if they have to write a check or two to settle lawsuits,” Yarbrough said. “But I don’t want to scare anyone out of using e-mails. Electronic communication is such an integral and important part of how we work and conduct business today. The point is to use e-mail intelligently and just take a little time to think about what you’re putting into those messages before you hit the ‘send’ button.”

Because once an e-mail is sent, it is out there in cyberspace forever.

Bill Leonard is senior writer for SHRM.

Society for Human Resource Management

1800 Duke Street
Alexandria, Virginia 22314 USA

Phone US Only: (800) 283-SHRM (7476)
Phone International: +1 (703) 548-3440

TTY/TDD (703) 548-6999
Fax (703) 535-6490

Questions? Contact SHRM
Careers Careers @ SHRM

\n\n\n"); ubertags_renderMarkup(container, bezen.nix);

\n"); ubertags_renderMarkup(container, bezen.nix); \n\n\n"); ubertags_renderMarkup(container, bezen.nix);