Message Logic®
intelligent message archiving

7 Mistakes You Can Avoid with Email Harassment Cases

Data Storage Corporation
Excellence in Data Protection and Recovery

Message Logic is a business unit of
Data Storage Corporation. 212-564-4922
www.messagelogic.net or www.datastoragecorp.com

In its landmark 7-2 decision, the U.S. Supreme Court ruled that employers are responsible for harassment — even if they are not aware that it is going on. Specifically, employers may be held liable if the employer “should have known of the conduct and fails to take immediate and appropriate corrective action.” (Burlington Industries v. Ellerth and Faragher vs. City of Boca Raton)

The “should have known” standard is particularly trouble- some when harassment involves email. How can a company know about every email message from its employees when thousands of messages are sent every day? Which messages should the company know about?

The liability for not knowing about email harassment can be substantial. While most harassment cases are settled out of court with a confidential result, a few well-known cases that centered on email show the size of risk to business:

• Congressman Mark Foley of Florida abruptly resigned as the result of emails and instant messages he wrote to a former teenage male page.

• Chevron paid $2.2-million to four female employees to settle a lawsuit in which they claimed they were sexually harassed with email jokes.

• Two African American Morgan Stanley employees filed a $60 million racial discrimination lawsuit claiming racist jokes were disseminated via email. The case was settled for an undisclosed sum.

The good news is that the U.S. Supreme Court said that penalties and fines could be lessened if the companies exercised “reasonable care” to prevent and correct harassment. (Burlington Industries v. Ellerth and Faragher vs. City of Boca Raton)

Many harassment suits are now focused on whether companies exercised “reasonable care.” Many companies compound their risk by the mistakes they make when handling email. Fortunately, there are steps that you can take as part of your overall anti-harassment program that may help.

Mistake 1: Ignore Email in Harassment Training and Policies

Email and internet abuse are responsible for more disciplinary actions than dishonesty, violence, and health and safety issues combined, according to a U.K. survey by *Personnel Today* magazine and KLegal (a legal firm associated with KPMG). Yet many employee harassment training programs and Personnel Policies do not specifically discuss the risks inherent in email use.

It makes sense to communicate how email is a permanent record, unlike phone and water cooler conversations. An employee’s words, which may seem like a joke between colleagues, can take on a totally different meaning when made public.

In 2001, the CEO of Cerner Corp. sent an email message to his management team berating them for creating a corporate culture in which parking lots were empty before 8 a.m. and on Saturdays.

He said, “Hell will freeze over before this CEO implements ANOTHER EMPLOYEE benefit in this Culture.”

Instead of remaining within the management team, the email was posted on Yahoo! Excerpts from the message were prominently printed in the Wall Street Journal and the New York Times. Cerner stock quickly plummeted about 25%.

RECOMMENDATION: Review your current harassment training and published personnel policies with a qualified legal professional. Make sure to include references to what could happen to messages in the hands of a plaintiff's attorney or printed in the press. Demonstrate by using examples of actual email messages.

Mistake 2: Delete Email Frequently

Some managers believe it is best to frequently delete all messages from the corporate email server. They claim it's impossible to establish a pattern of wrong doing if the mail does not exist.

Unfortunately, even if a message is deleted from the corporate server, an exact copy of an incriminating email may be in various desktop computers, printed paper, BlackBerry, handhelds or the email server of an ISP.

In hostile workplace cases, the courts have allowed plaintiffs to introduce printed copies of provocative emails even though the employer could not locate a record of these messages in its system. (Schwenn vs. Anheuser-Busch) In such a case, the employer cannot refute the evidence.

Missing email can also impact the case even if the plaintiff does not have a printed copy. The largest single sex discrimination verdict in U.S. history, $29.2-million, was awarded when the company could not produce copies of relevant emails. As records may have been intentionally deleted, the court instructed the jury to assume that the lost emails would have been unfavorable to the defendant. (Zubulake vs. UBS Warburg)

RECOMMENDATION: It is critical to be able to promptly recover messages when needed. At a minimum, system back-up tapes make it possible to recover messages.

However, significant effort is required to re-build an email file from back-up tapes. It is better to have a "searchable archive" of messages that allows you to quickly find messages by sender, receiver, and message content. It will also allow you to filter the results by date.

Mistake 3: Wait for a Complaint

Even when there was substantial evidence, including a significant number of email messages that could have led to a hostile work environment, the court ruled that a hostile work environment did not exist on the grounds that the employer had taken prompt remedial action when it learned of the emails. (Knox vs. Indiana)

But, if a court rules that you "should have known" about harassing emails and did not, you cannot take prompt remedial action in time. In a similar case, the New Jersey Supreme Court ruled unanimously that an employer could be liable for a hostile work environment based on what was posted in an electronic bulletin board even though nobody had complained. (Blakey vs. Continental Airlines)

In addition, in a case where you have taken disciplinary remedial action, it is important to proactively know if the violations continue to take place. If you fail to monitor email and an additional complaint is made, you can be open to charges that your remedial actions were not sufficient. It is important, therefore, to promptly learn of possible harassment. Sophisticated monitoring systems are available to sort messages and to notify key personnel of potential risks. You want a system that can identify messages that can lead to a hostile work environment case and one that can specifically monitor the email of employees against whom a complaint has been filed. Some of these tools can provide immediate notification to a compliance officer, human resources professional, or company executive when a potentially risky message is sent.

As these monitoring systems become more commonly deployed, it may be possible for a plaintiff to establish that a company "should have known" about offensive email because the technology to detect them was readily available. Failure to deploy these products may increase your risk.

RECOMMENDATION: Deploy a monitoring system that can provide real-time alerts and daily summaries. Consider
a system that can segregate alerts by department manager or message type.

For example, an alert for harassment may be sent to a human resources professional and other alerts may be sent to the IT department.

Mistake 4: Monitor Only External Email

Sixty percent of companies monitor external (incoming & outgoing) e-mail as a way to protect against intruders, leaks, and offensive content. However, only 27% monitor internal messages (employee to employee) where harassment is likely to take place. (American Management Association/ePolicy Institute 2004 survey)

"Management's failure to check internal e-mail is a potentially costly oversight. Off-the-cuff, casual e-mail conversations among employees are exactly the type of messages that tend to trigger lawsuits and arm litigators with damaging evidence", said Nancy Flynn, executive director of the ePolicy Institute, in a press release.

The reason is that many of the products in the market are designed for other tasks. For example, some companies with anti-spam firewall products use the same technology to monitor outbound mail. The largest problem is that spam products are designed for external attacks and are often installed where the corporate network meets the Internet. Another problem is that spam lexicons are designed to catch many things, including financial offers, pharmaceutical products, and other things that would not lead to harassment.

RECOMMENDATION: Avoid monitoring systems that install only between your email system and the Internet as they may not catch employee-to-employee mail. Such products may work only on communications "entering or leaving the corporate network." Often the products to
avoid will use terms like "perimeter systems", "firewalls","gateways", or "servers". Look for products that are specifically designed for internal mail.

Mistake 5: Focus on Individual Messages Instead of Trends

Many email monitoring products do not keep copies of messages processed or the decisions made by the product. This is because many of the monitoring products are based on anti-spam products that do not need to keep a copy of good messages and may delete spam after a short quarantine period. Because they don't store messages, these products do not include rapid search capabilities because the designers of the original anti-spam products did not anticipate that anyone would ever do a search of spam.

In establishing a defense for hostile work environment, it is important to be able to identify trends and to locate messages that might include mitigating factors. Some key questions include:

- Who are the top senders of offensive messages?

- Did a person who sent an offensive message to person "A" send offensive messages to anyone else?

- Did person "B" receive any new offensive messages, especially after the company was notified of a complaint? (A potential key issue in determining whether the company used "reasonable care" to fix the problem.)

The best monitoring products keep copies of all messages for a period of six months or more so that trends and past actions can be analyzed.

They will allow you to sort messages by sender, recipient, and whether or not a message contained offensive content.
The best systems have an easy user interface that can be accessed using a web browser and without intervention by the IT department.

RECOMMENDATION: Find products that both provide real-time alerts and keep messages for further analysis. Copies of the decisions made by the product and the ability to easily search past messages are important features.

Mistake 6: Depend on Lexicons to Find Harassment

Lexicons are lists of words and phrases. The initial response of many people who need to find harassment is to search for messages using a lexicon of dirty words. Other companies may extend the lexicon to include words for other forms of harassment, such as racial and ethnic slurs.

To examine the effectiveness of this lexicon approach, **Message Logic, Inc**. performed a study by applying these techniques to 517,403 email messages obtained from the U.S. investigation of Enron Corporation. These messages represent messages from key executives and professionals over a two year period of time.

When most people first try to find harassing email messages within a large body of messages they usually start by searching for dirty words and phrases. They quickly realize that additional types of words and phrases, such as ethnic slurs, need to be added, but eventually four problems emerge:

- They cannot think of all of the possible words and phrase combinations.
- They realize that some offensive words also have non-offensive meanings. The result is that the search yields many messages that are not actually harassment.
- They discover that as the list gets longer, the processing time to compare each message to the list gets longer.
- They discover that some messages that do not have any offensive words within them could be used as evidence of a hostile work environment.

Message Logic uses a more advanced, proprietary technique to find potentially harassing messages. These methods are primarily based on statistical language models. **Message Logic** assembled tens of thousands of messages from many companies and sorted them in terms of whether they contained potentially inappropriate content. We built statistical models of these messages to find which words and other elements are more commonly found in risky messages and which are more commonly found in messages that are not offensive.

To analyze a new message, **Message Logic** compares the message to the language models and performs a complex analysis to see if it is potentially harassing.

While examining products, be sure to look beyond the claims. Be especially skeptical of the products from companies that claim that they spent years working on lexicons, word lists, and phrases. Ask for proof that the Solution would catch these examples and others like them.

It is clear from our analysis that finding potentially inappropriate messages using just offensive words misses a significant number of messages. In the case of
the Enron messages, the lexicon method missed 33% of the messages that need review. Stated another way, the lexicon approach missed 3691 messages, or about 7 out of every 1000 messages.

The best results come from a combination of lexicons with language technology. While no method, including human review, is perfect, the combination of lexicons with language technology optimizes the chances of finding the messages in a timely manner.

RECOMMENDATION: Do not depend on key words or lexicons alone to find harassment as a significant number of potentially risky messages are missed. Look for systems that combine lexicons with statistical language models.

Mistake 7: Use Products That Do Not Adjust To Your Culture

Any organization can be on the receiving end of a hostile work environment complaint. However, the standard of what constitutes a hostile work environment may differ by the organization or the geography. For example, a Las Vegas nightclub may have a different standard for what constitutes harassment than an elementary school.

The best systems allow you to adjust the sensitivity of the harassment filters to your organizational needs. These adjustments may need to be updated depending upon changing circumstances without involving the vendor.

RECOMMENDATION: Find a monitoring product that allows you to adjust its sensitivity based on the needs of your organization without the need to contact the vendor.

Conclusion

It is difficult to know when an employee sends an email that could become evidence in a hostile work environment case. However, the high “should have known” standard created by the U.S. Supreme Court means that companies need to be proactive. When determining whether a hostile work environment exists, courts may consider whether a company took “immediate and appropriate corrective action.”

Various products, such as **Message Logic**, are available as part of your overall anti- harassment program to monitor messages and to alert you to potential problems. When being proactive, it is important to consider the following key factors:

1. Include email in your policies and as examples in your training.
2. Archive your emails so that you have a record of what was sent.
3. Proactively monitor messages with flexible alerts for immediate action.
4. Make sure to monitor internal email as well as external email. Most employee-to-employee communication will be internal.
5. Identify trends with tools that can easily search archived messages and enable you to find frequent senders of offensive content.
6. Use advanced statistical technologies, not just lexicons and word lists, to maximize your chance of finding offensive messages.
7. Deploy only products that can adjust to reflect your corporate culture.