



Monsters In Your Mailbox

Email Liability, Compliance, and Policy Management Risk; A Case Study of the Enron Corporation

**By Roger Matus, Chief Executive, and Sean True, Chief Technologist,
InBoxer, Inc.**

Anyone can send an email message. Unfortunately, at most companies, that means that everyone has the ability to use email to give away company secrets, harass fellow employees, or violate the privacy provisions of laws like HIPAA and Gramm-Leach-Bliley. Even though such actions may be unauthorized, the fact that these messages can be sent from an official company email address puts employers at risk.

The statistics are staggering. Ninety percent of employees admitted to using company email for personal use; about 60% disclosed sending adult email at work, including jokes; and 50% said they received racist, sexist, pornographic, or otherwise disparaging email at work (Source: AMA/ePolicy Institute). Twenty-seven percent of Fortune 500 companies have fought harassment claims involving email (Source: IDC). And, in a survey released in 2004, more than 20% of all employers have been ordered to produce employee email in the course of a lawsuit or regulatory investigation (Source: AMA/ePolicy Institute).

Violations may result in large fines or settlements. Here are two examples:

- Norwich Union Insurance (UK) paid a competitor £450,000 to settle a case of defamation by email against a competitor, Western Provident Association. The award was based on a single internal email message that somebody forwarded outside of the company.

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

One does not need to be guilty to pay a high price. The process of producing emails for review in response to a discovery process or an investigation can include hours of legal and IT expenses. The indirect costs of damage to a company's reputation if the messages become public may be even larger.

What is My Liability Risk?

To understand the extent of the email liability risk to an enterprise, InBoxer, Inc. embarked on a detailed study of email messages from one company, using sophisticated new language-based analytical tools based on its InBoxer® anti-spam software.

While there are many visible examples of problems caused by email risk, until now it has been impossible to know whether the penalties resulted from a small number of messages at selected companies or a more systemic problem. Of all the messages sent by the employees of a company, how many could cause a problem? Such a research project would require hundreds of thousands of uncensored messages collected over a long period of time from people who did not know that they were being watched. Originally, it was difficult to find a company willing to surrender

so many email messages for such careful scrutiny. But one company's misfortune made this research possible.

As part of the investigation of Enron Corp., the Federal Energy Regulatory Commission (FERC) seized Enron's Outlook email database. On March 23, 2003, nearly 1.6 million emails, tasks, and calendar entries, written during 2000-2002 by 176 former Enron executives and employees from the power-trading operations were released to the public. This was the first public release of such a broad corpus of email messages and provided an ideal subject to use for this research.

By all conventional signs, Enron was the epitome of a respected, successful enterprise. In one decade it grew from a natural gas pipeline operator into an energy trading giant, reaching seventh on the Fortune 500. The company certainly had the ability to train employees about the proper handling of confidential information and respect in the workplace. One could assume that senior employees were well intentioned and had the best interests of Enron in mind. There would be no reason to suspect them of unusual behavior or deliberate email sabotage.

Confidential, Personal Records

FERC originally released all of the messages, tasks, and calendar entries. The records were posted on the Internet for all to search. These included confidential personal information such as bank records, social security numbers, birth dates, and performance reviews. One message contained an attachment listing the salaries and social security numbers of every employee.

It was reported, although not confirmed, that information from the release of this information was used as evidence leading to a divorce and that salary information was sent widely to disgruntled employees.

The release of these emails also raised the very real risk of identity theft and, in the eyes of some, potential harm to children who were named in family email messages -- along with personal information such as their ages and day care schedules.

Enron employees whose emails were released pleaded for their confidential personal data to be removed. In response, the database was taken off-line for 10 days. One hundred Enron employees, mostly from the human resources department, reviewed the 1.6 million entries. To save time, the Enron team searched the documents using key word searches with terms like "kids," "divorce," "social security," and "credit card number" to identify records to be removed.

As a result, 9% (141,379) of the documents were removed from the database and then only the remaining documents were re-released. It is believed that the removed documents contained specific confidential information and not just embarrassing information. However, they were not available for further analysis.

Of the roughly 1.4 million documents remaining, calendar entries, tasks, and other administrative tracking messages were removed. Various data integrity problems were resolved, utilizing work done by the Massachusetts Institute of Technology, Stanford Research Institute, and Carnegie-Mellon University. The remaining corpus was 517,403 email messages -- ample for a valid analysis.

Non-Business Content vs. Business Content

The first objective of this study was to identify email that was not related to the company business. Many employees use email for casual purposes, much in the way they might communicate to friends and co-workers on the phone or in person by the water

cooler. The problem with email is that the content does not contain personal clues, such as tone of voice, which may indicate intent. In addition, as email is more permanent than verbal conversation, content found later may be taken out of context.

There are two specific business issues with non-business email: (1) Recipients must try to distinguish between a personal request and an official request. For example, is a message from a member of the management team a demand or a personal request? (2) Companies are required to store business records, including emails. Sometimes these messages must be kept for years. Is there a way to separate the non-business mail so that these messages do not clog the email archive?

At the start of the analysis, the InBoxer team was unsure of what to expect. Would the data be useful without the personal content? Were Enron employees well trained about what to commit to writing? Then, the team saw the first record made available by FERC. It contained the embarrassing statement: “So . . . you were looking for a one night stand after all . . . ??” It was clear that all types of messages might be found.

```
SDOC_NO = 1
FROM: Dawn C
TO: Bill W
DATE = 11/26/2001
TIME : 16:23:24

So ... you were looking for a one night stand after
all ... ??

DC
```

Figure 1. The first email in the Enron database made public by the FERC (Last names removed by the authors.)

A systematic analysis of all the available email messages was then performed. The team processed the available 517,403 messages, using the InBoxer language analysis tools. The InBoxer-based tools analyzed the text of the messages and sorted them into “personal vs. business.” Its language model identified

nearly 20% of the messages as having non-business content (98,873 vs. 413,526 messages).

The chart in Figure 2 shows the statistical distribution of the messages. Most of the messages, shown by the spike on the left, contained clearly identifiable business content. The messages identified by the spike on the right were identified by the tool as purely personal in nature. Only a few messages in the middle could not be classified as one or the other. That could be because those messages contained both business and personal elements, such as meeting a co-worker for dinner after a business meeting.

The chart shows a “U” shaped curve, which is close to ideal for analysis.

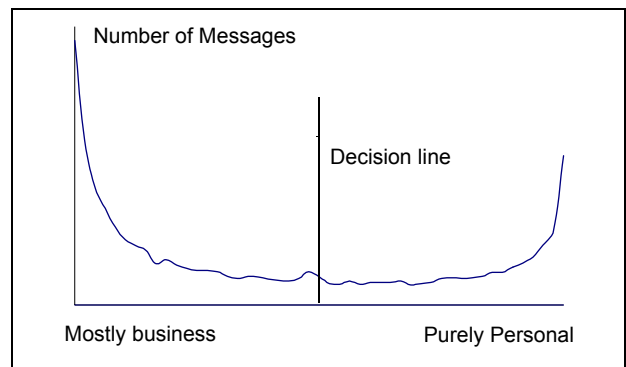


Figure 2. Distribution of Personal vs. Business emails

Non-business Messages

What types of non-business messages could lead to confusion by employees?

Figure 3 shows an email from an Enron executive that was sent to a very wide list of recipients. The names of the sender and recipients were removed or abbreviated by the authors, but they are clearly visible in the database. In the message below, Jim H. made statements about politics that could concern some employees or business partners. Does it express a personal or corporate opinion? The message was distributed widely and could have been forwarded easily.

Inappropriate Mail

```
SDOC_NO = 202924
FROM: Jim H
TO: (fairly large list)
DATE = 11/08/2000 TIME : 15:40:00
SUBJECT : RE: to my CA friends
. . . Right on, Gary. With all respect to our
California friends, this idea that "the right
Republican candidate" can win here is bullshit. ...
After four years in the SF Bay area, I am convinced
this state is most onesided [sic], narrow-minded,
anti-freedom place I have ever lived or visited.
And I don't think anyone ever considered me a right-
winger, but my God, I find myself so out of place
here, politically, that I am truly stunned! I
actually had a group of people in a park walk away
from me when they found out my dog's name was
```

Figure 3. Email with confusing personal or corporate content

Figure 4 contains a directive from an executive at Enron that demands that it be passed on to “all your friends.” Was this a business requirement that could not be ignored? Is it possible that certain employees could feel that those who followed the instructions would get more favorable treatment than others? The message certainly conveys a more hostile work environment for Democrats than Republicans.

```
SDOC_NO = 895607
FROM: Eric B
TO: (fairly large list)
DATE = 10/23/2000 TIME : 08:26:00
SUBJECT : Fwd: Al Gore... By the Numbers
. . .
PLEASE PASS THIS ON TO ALL YOUR FRIENDS!
...
The average Republican has 28 names in his or her
email directory that means if we all forward this
message to our friends, this one email can reach 14
million citizens! Please forward to your friends
and make sure every online Republican signs up ...
```

Figure 4. Email expressing a personal request or requirement

Personal Messages

Other types of personal messages could embarrass employees. Figures 5 and 6 show messages that are clearly personal and do not contain any business content. Yet, they were available for investigators to discover. The first contains information about the stress level of and possible treatment for the Chairman of

the corporation. If such information were released in a timely manner about a public company, it could have an impact on the stock price. The second is a more private message about a personal relationship problem that could embarrass both employees.

```
SDOC_NO = 1445175
FROM: "Linda P. Lay"
TO: Kenneth L. Lay
DATE = 10/30/2001 TIME : 09:44:07
...
-----Original Message-----
From: Phyllis B
To: Linda Lay
Subject: RE: Biochemical Research Foundation

Dear Linda,

...
I am concerned about his (Ken's) level of stress,
and would highly recommend that he keep up that
anxiety control formula, taking two after meals 3x
a day. I have stronger things in my arsenal if
needed. Also, perhaps when he is here sometime, I
could check his blood chemistry for stress factors
and optimal brain function.
Warmest Regards,
Phyllis
```

Figure 5. Email with potentially embarrassing information about an executive

```
SDOC_NO = 179173
FROM: Jeff D
TO: Prentice S
DATE = 10/02/2000 TIME : 10:25:00
SUBJECT : Re: I'm sorry
Prentice:
I'm happy to talk. However, if you're unhappy
because 1) I haven't asked you to marry me, or 2) I
haven't asked you to move in together, or 3) I
haven't asked you to have children, then you need
to say so. ...
After this long, if you want to discuss my
dishonesty, then I think we need to take a hard
look at why we're in this at all. So I'm happy to
talk, but not on the phone, and not about who's the
bigger asshole, or who's a lying son-of-a-bitch.
```

Figure 6. Email containing personal information that clearly should not be made public

Inappropriate Mail

Beyond personal mail is the category of “inappropriate mail.” These messages are not only inconvenient,

but could lead to charges of a hostile work environment, harassment lawsuits, and other harmful actions. Earlier, it was mentioned that 50% of those surveyed by the AMA/ePolicy Institute said they received racist, sexist, pornographic, or otherwise disparaging email at work. However, did each person receive only the occasional message or was the problem more widespread?

The InBoxer study showed that about 4% of the messages (20,378) in the Enron database contained pornographic content, racially or ethnically offensive language, dirty jokes, or questionable images. Any one of these messages might have been actionable. The fact that nearly 1 out of every 25 messages in the database could have been a problem was seen by the InBoxer team as a warning for businesses.

The distribution of emails by the InBoxer analysis is shown in Figure 7. The spikes on the left and right of the chart show that it is clearly possible to identify the inappropriate content using the InBoxer tools.

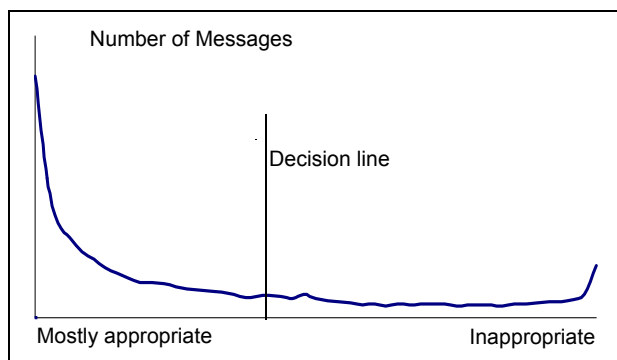


Figure 7. Distribution of Mostly Appropriate vs. Inappropriate emails

A detailed look into the messages showed that the inappropriate mails were often blatant. Many of the messages contained inappropriate images that were pornographic or otherwise offensive. While it is not appropriate to display those messages here, a sample of some of the message subject lines provides insight into the nature of the messages:

- Palm Beach Voters

- Chick from Sask
- The new Democratic seal
- Afganistans First Missile [sic]
- Redneck classifier
- Redneck horseshoes
- Lonely?
- XXX Cartoons
- Martha Stewart Holiday Trip

The message in Figure 8 is a mild example of adult content in an image. While the image is not explicitly pornographic, it may be seen as offensive by many people. Such an image can be used as evidence of a hostile work environment. This particular image, under the subject “Your son's first NFL game” was widely forwarded and re-forwarded.



Figure 8. Adult content, even when not sexually explicit, can offend employees and create a hostile work environment (bar added by authors)

The authors were further shocked by the extent of the problem in some messages. The message shown in Figure 9 is a particular example. It is clearly racist and offensive to large numbers of people. The text content is about deadbeat fathers, but includes an image of a well known and reputable civil rights leader superimposed on a young girl's face. The intent is to suggest that this leader is the father of such a child. Messages like this, sent from an official corporate email address, can lead people to believe that the company is not welcoming to minorities.

Result of the Study

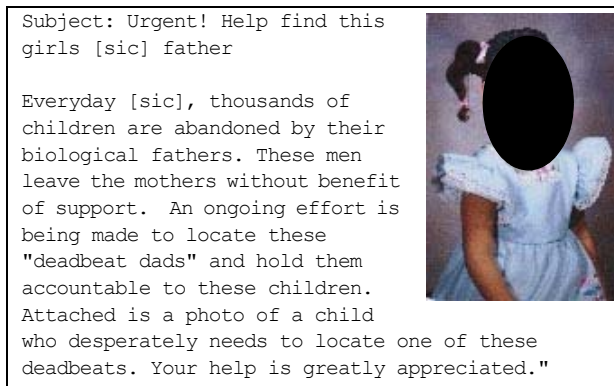


Figure 9. Racially offensive and inappropriate (circle added by authors)

Explicit and offensive language creates another kind of risk. Not only might such messages offend individuals, but they can be very demoralizing to recipients. The message in Figure 10 was forwarded several times. It appears to have been sent by Jeff Skilling, Enron president, but it could be an impersonator.

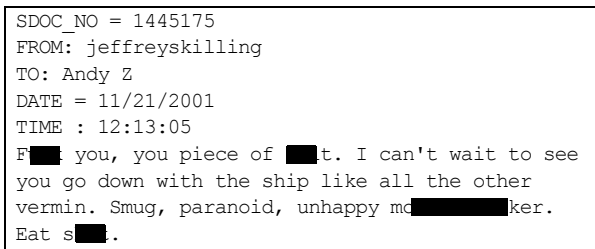


Figure 10. Offensive language purportedly written by an Enron executive (bars added by authors)

Jokes are another kind of offending mail. Often, they are a part of the company culture. However, jokes that are at the expense of classes of people may give the impression that the company believes that certain classes of employees are less valued than others. Many of the jokes in the Enron database related to politics (specifically about members of the Democratic Party) and about women. Figure 11 contains an example of one of the milder jokes involving women.

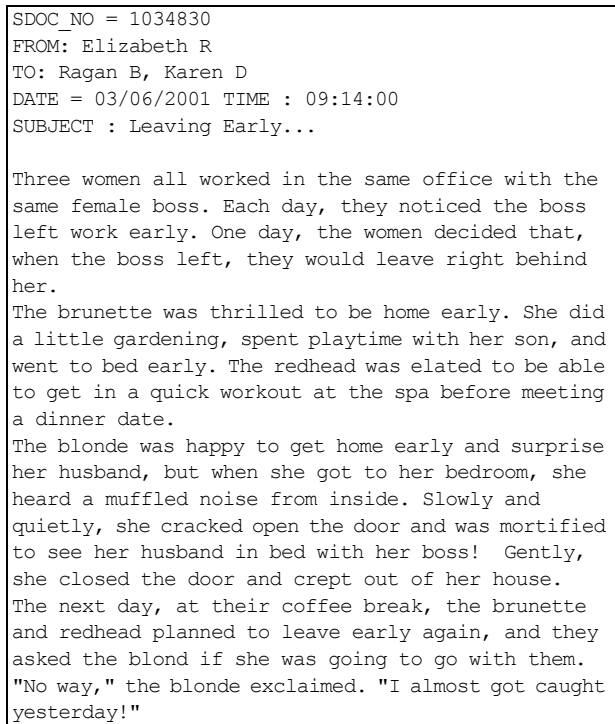


Figure 11. One of many jokes circulated via Enron corporate email

Result of the Study

The InBoxer analysis of Enron emails reveals email risk is not the result of one or two messages in an organization. The number of messages is large, the types of problems are broad, and the number of people involved in sending questionable content crosses the company. Some of the specific details from the study are as follows:

- Nine percent of the messages in the overall database (141,379 out of 1.6 million) contained personal, confidential information that was so sensitive that it had to be removed from the database.
- Nineteen percent of the messages (98,873 out of 517,403) available for analysis were personal in nature. They could have been confusing or embarrassing because they came from an official email address.

- Four percent of the messages (20,378 out of 517,403) contained inappropriate content such as pornographic content, racially or ethnically offensive language, dirty jokes, or questionable images.

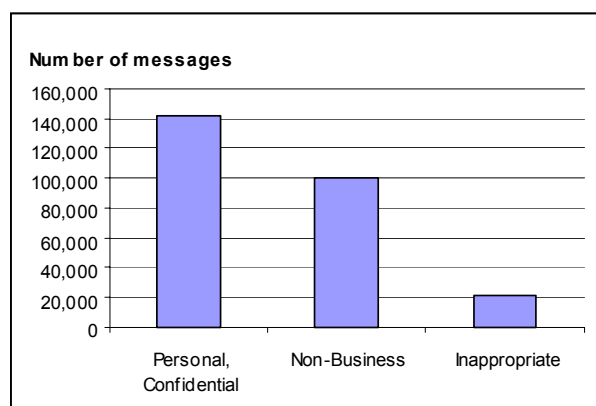


Figure 12. Message count of analyzed message by category

Other critical risks were not evaluated, including theft of intellectual property, violation of business confidentiality, and regulatory storage requirements.

In retrospect, it may be said that the Enron corporate culture was extreme. However, the company was well respected and its valuation was quite high. Workplace lawsuits and studies (such as those mentioned at the beginning of this paper) also indicate that Enron is not an isolated case of email abuse.

As a result of this case study, the authors believe that the risk of corporate email liability is significant. Organizations need to institute policies and take steps to manage the risk of email. InBoxer, Inc.

is developing a software product based on the language technologies used in this study. The goal is to help companies reduce their liability risk by advising the sender of some potential problems *before* a message is sent. It will behave like a spelling checker, except that it checks outbound messages for liability, compliance, and policy management concerns.

The InBoxer tools and methodology can be deployed immediately for a custom analysis on a confidential basis. Such research can determine the extent of the risk facing an organization and can identify the types of risks that the organization is facing.

For further information on performing such an analysis contact the authors at info@inboxer.com or call 1-617-499-7700 (in the U.K. call 0871-733-6293).

Copyright 2005 by InBoxer, Inc. All Rights Reserved.

Not responsible for errors. Subject to change without notice.

INBOXER and AUDIOTRIEVE are registered trademarks and the INBOXER logo is a trademark of InBoxer, Inc.

All other marks are property of their respective owners.

For further information, please visit www.inboxer.com, write info@inboxer.com, or call 1-617-499-7700 (in the UK call 0871-733-6293)