Privacy, Ethics and Embarassment
Full Version of the Abbreviated CSI April 2006 Alert Version
Rebecca Herold, CISSP, CISM, CISA, FLMI
March 2006

Businesses Need to Have a Conscience

One of my favorite movies of all time is “It’s a Wonderful Life.” A scene that still resonates with business today is when Mr. Potter offers George Bailey a high-paying job. George is amazed and flattered with the offer considering how much more money and prestige it will bring him until he shakes Potter’s hand; he can feel it isn’t right, rubs his fingers together as though he’s feeling the oily residue that has rubbed off of Potter’s unethical soul onto his hand, and you can see on his face that he realizes he is being manipulated by Potter, the “scurvy little spider.”

In January I got an unsolicited package in the mail from a security software vendor, whose name I will not promote here. I opened it up, and there was a copy of Enron's 2000 "Code of Ethics" booklet, which also contained the corporation's information security policies. This surprised me. Hmm; what was this all about?

Reading the letter I found that this vendor was promoting their product by encouraging potential customers to view a site they set up with a copy of all the Enron email messages, "over 85,000 records" that were on the Enron system at the time of the Enron collapse and sending the Enron policies to demonstrate the noncompliance. The vendor tried to rationalize this by indicating that since the information "is already posted on the web by the Federal Energy Regulatory Commission" that the vendor "believes that it is not harming anyone." However, right before this the vendor indicated that it, "believes that most Enron employees are (and were) hard working, honest people who are (and were) trying to do a good job. We respect them and apologize for any embarrassment that this content may cause them." They have documented that they realize they are probably embarrassing or harming someone by their actions.

Embarrass A Person TO Win A Prize!

The vendor then goes on to offer three separate contests, each with a prize of iPod shuffles, to the people who, after searching through the Enron emails, can find the best emails that 1) would be grounds for firing, 2) contained the funniest jokes, and 3) were the most embarrassing to the sender. So, they are now encouraging others to further embarrass the people named in the emails.

The vendor indicated it had scrubbed the emails of "really personal information." However, all the people's names, first and last names, are clearly seen in the text that the people in the contest have submitted onto the vendor’s site that were copied from the Enron email database. Gee, full names, are rather personal, don't you think? Also, how was “really personal information” actually removed from the 85,000 messages? If they had really removed such information would there have been any information left to support their contests?

Does this feel right or ethical to you? As I read the letter I felt as though I had just shook hands with Mr. Potter. It is one thing for the government to post

evidence under public access laws, but it quite another thing for a vendor to actually make a copy of the information and post it, stating that they realize their actions will cause embarrassment to the people named within the emails, people who have lost their jobs and life savings, probably many people mentioned who weren't even employees at Enron, solely for the purpose of promoting the vendor's security product. And then to go on to have three separate contests encouraging the public as large to continue to embarrass them is really the icing on the cake!

There were around 28,000 Enron employees who lost their jobs, in addition to another 85,000 Arthur Andersen employees who also subsequently lost their jobs. And now the vendor is taking opportunist advantage of the situation, and government regulations regarding evidence, to blatantly promote their security product and even go a step further and explicitly embarrass anyone named in the now "public" documents in the name of their marketing gimmick...just because they can…and it will help their sales.

It is like this vendor set up a circus around a train wreck and created carnival side shows around the scattered victims. Does this seem right to you? Does this seem ethical? If the vendor has CISSP, CISM, CISA or other certified professionals in their staff who went along with this, are they in violation of their codes of ethics promises?

The Enron trial started January 31, 2006. I'm sure the Google searches on information related to it are high. I'm sure this vendor had a very high hit rate on their site. No, I did not search the email database at their site; their justification for doing the macabre marketing stunts were disgusting. The longer you think about this the more your gut, heart and conscience should tell you this is wrong.

It is ironic that an organization in court for being so unethical now has other organizations doing actions that are also ethically questionable. It is similar to the mob mentality, isn't it? If someone else is doing bad things, then others will often join in just because they think they won't get singled out and will in fact get some benefit from it.

Aren't Teddies Fair Game?

Why should organizations worry about revealing personal data if doing so does not explicitly break any regulations? If it would take human and dollar resources to make the changes necessary to protect the non-regulated personal data, then why do anything? Well, some of you probably think I've already beaten the ethics reasons to death. So, consider the potential negative business impact along with the embarrassment factor of the individuals involved.

Recall the incident that occurred with Victoria's Secret in 2002. An error within their website application code allowed visitors to the site to be able to view all the other customers' orders, including their full names and the specific types of

intimate apparel they had purchased. Very embarrassing indeed for many of the customers! This information could also have been copied onto other sites, prolonging the embarrassment factor long after the application was fixed. The customer information could also have been obtained by other organizations and used for their marketing campaigns.

It was widely reported that the problem was not fixed right away after a customer notified the company; there were no laws or regulations explicitly requiring the data available for viewing to be secured. True, it is doubtful there is any law explicitly requiring information about teddies and thongs to be protected. However, the programming flaw was fixed after publicity regarding the incident occurred. The incident was viewed as an incident of gross privacy invasion, and also a violation of the company's posted privacy policy. Under the settlement, Victoria's Secret had to compensate New Yorkers whose personal information was accessible via the Internet, pay a $50,000 fine and implement a series of improvements for their website security.

Even If It Isn't Illegal, Actions Perceived As Unethical Hurt Business

Embarrassment resulting from privacy invasions of personal information that may not be covered by any specific laws certainly can have an impact on organizations. Embarrassment is a component of privacy that often gets overlooked by organizations that are focusing only on the "letter of the law" for what is legally allowed when handling personal information and when trying to get an edge on the competition. Not only can the resulting legal actions impact a business, but the damaged reputation and lost customers resulting from the bad publicity and perceived callousness could have a much longer-lasting impact. Using personal information in ethical ways, in addition to ways that comply with the law, are ultimately good for business.

After a presentation I did on privacy at a conference some time ago, one of the attendees chatted with me for a while afterwards about the use of "found" personal information. During the presentation I had talked about the importance, particularly for international data protection law compliance, of getting consent from individuals to use their personal information. The attendee indicated his marketing area had figured out a way to harvest the names and contact information from unprotected retail web servers and include them within their marketing databases. There was no law against this, was there, since the individuals had probably consented to having their information collected by those web servers for marketing purposes? Hmm…interesting logic. Be very, very careful. If I give my consent to Company X for them to use my personal information it does not mean I have not consented to having every other Company Y and Z deluge me with their marketing arsenal.

Greed is Good!

Today, the ease of collecting and disseminating personal information is unprecedented. Yes, legally, in the United States at least, individuals have a

right to view databases of public records, which the Enron emails have become as an affect of being evidence for the trial. Technologically it is easy to post them on the Internet. But just because it can easily be done does not mean it should be done.

Unguarded moments, careless words of youth or naivety, or even messages spoofed by others, can now be viewed by an audience of millions, following those victims for years to come. Recall the 15-year-old known as the Star Wars Kid. He became famous because a video of him was posted on the Internet as a joke; reportedly causing the young man considerable embarrassment and raising many privacy discussions. The video remains widely circulated and will be something that will follow him the rest of his life. The people being made the butt of jokes in the Enron emails will quite possibly impact them the rest of their lives. But, the vendor is getting good publicity at their expense, and it is not breaking any law, so that makes it okay, right? Well, they are certainly getting publicity, and many organizations may decide they do not want to do business with such an organization.

This reminds me of the quote from the1987 movie “Wallstreet” with Michael Douglas and Charlie Sheen, “Greed is good!” It is sad that this motto is paid homage to by organizations through the use of public access laws and exploiting the misfortunes of others, to ironically promote an information security and privacy product.

Even if you can use “found” personal information with potential financial gain without breaking any laws, should you? Well, Mr. Potter kept his found money from the trashcan in his bank, knowing, and delighting, in the harsh impact his actions would have upon George Bailey and many others in Bedford Falls and how it would financially benefit him. Do you want your organization to follow a Mr. Potter ethics example?

Rebecca Herold, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and adjunct professor, and can be reached at rebeccaherold@rebeccaherold.com. Rebecca has an M.A. in Computer Science & Education, and authored books including “The Privacy Papers,” “Managing an Information Security and Privacy Awareness and Training Program,” and “The Privacy Management Toolkit.”

