

This is Google's cache of http://www.odwyerpr.com/members/0205comm_nicolazzo_breaches.htm as retrieved on 11 Feb 2007 04:54:15 GMT.

Google's cache is the snapshot that we took of the page as we crawled the web.

The page may have changed since that time. Click here for the [current page](#) without highlighting.

This cached page may reference images which are no longer available. Click here for the [cached text](#) only.

To link to or bookmark this page, use the following url: http://www.google.com/search?sourceid=navclient&ie=UTF-8&rls=GGIH,GGIH:2007-02,GGIH:en&q=cache:http%3A%2F%2Fwww.odwyerpr.com%2Fmembers%2F0205comm_nicolazzo_breaches.htm

*Google is neither affiliated with
the authors of this page
nor responsible for its content.*

Contact O'Dwyer's: 271 Madison Ave., #600, New York, NY 10016; Tel: 212/679-2471; Fax: 212/683-2750



ODWYERPR.COM > PR Commentary

[return to main page](#)



Richard E. Nicolazzo is president and CEO of Nicolazzo & Associates, a strategic communications and crisis management firm headquartered in Boston, Mass.

Feb. 5, 2007

SECURITY BREACHES:

LACK OF COMMUNICATION IS GIVING CONSUMERS THE SHAFT

By Richard Nicolazzo

Has anyone noticed a disturbing pattern in security breaches at major U.S. companies?

Due to slow – and even deliberate – delayed communications, consumers are getting the shaft.

The most recent case flared up in mid-January when TJX Cos., a Framingham, Mass. retailer that runs T.J. Maxx, Marshalls, Home Goods and other stores, [disclosed a data theft that exposed millions](#) of customer credit and debit card numbers.

Like several past instances, consumers were NOT notified right away. In the case of TJX, the company waited about a month. A couple of years ago when [Bank of America had some computer tapes stolen](#), it waited two months to notify customers.

Even the U.S. government [waited several weeks before disclosing](#) someone had walked off with a government-owned laptop containing Social Security information for 25.6 million U.S. citizens.

Corporate executives, government investigators, and legal counselors have been postulating that the communication gap exists because it gives the authorities time to catch the bad guys.

This may sound good on paper, but it doesn't do much for the consumer.

I'm in agreement that the ultimate objective is to catch these thieves and throw the book at them. However, companies are bucking a clear trend: the customer (in this

Companies are risking major damage to their reputations, brands, or even a substantial drop in sales.

OMEGA
WORLD TRAVEL



Gloria Bohan,
President & CEO

Over 200 Offices
Worldwide

Woman Owned
Founded 1972

Contact Us Today
212-563-3500
800-545-1003

case the consumer) comes first.

Take a closer look at the TJX case.

According to [a report in the Boston Globe](#), a New Bedford, Mass., city employee said \$6,700 in charges suddenly appeared on his Visa card in January of 2007. It's the same credit card he used while shopping at a T.J. Maxx store last December.

Does TJX really think it utilized the right communications strategy by waiting a month to tell this consumer about the breach? If you were this shopper, what would you think about TJX?

Could it be that TJX did not want to announce the breach in December because it would have severely impacted its Christmas sales?

My 30-plus years experience in strategic communications tells me this dynamic must change.

By waiting to tell the consumer about breaches, companies are risking major damage to their reputations and brands and even a substantial drop in sales.

While it's true that banks and other credit card issuers usually pick up the tab for bogus charges, there is still a huge psychological impact on the consumer. People whose personal data is stolen feel violated.

It may be gradual, but the American public is going to stand up against this behavior and demand to know right away that someone has stolen their financial data. At some point, it seems logical that consumers will organize boycotts against companies that compromise their personal data.

To make matters worse, some companies are making security breach announcements without solid contingency communication plans in place to deal with the fallout.

At the risk of picking on TJX, the company seemed disorganized when the story broke. People complained that they got the run-around from customer service hotlines and the CEO was unavailable for comment.

Finally, after more than two weeks, the company took full-page ads in newspapers saying that it was sorry for the inconvenience to consumers and it was doing everything in its power to correct the problem.

If the company had a good contingency communications plan in place, it would have called for a letter like this to be written within a matter of days. Why wait? It looks like the company is hiding something.

I believe there is an Rx to contain - and even fix - this problem. It involves work on the front end and the back end.

On the front end, organizations holding the data need to build more secure systems to protect consumer information. This will involve more capital spending on encryption, security software, and other various IT tools.

On the back end, state and national political leaders need to introduce legislation that compels companies to notify consumers within five days of a security breach. There will be opposition, but it's the right thing to do.

Meanwhile, all of us continue to hold our breath until the next security breach is

announced...and we wonder if our financial data will be compromised along with our credit standing and privacy.

* * *

Richard E. Nicolazzo is president and CEO of Nicolazzo & Associates, a strategic communications and crisis management firm headquartered in Boston, Mass.

[Archive of PR Commentary](#)

RSS

[return to main page of odwyerpr.com >>](#)

 [Click here to print](#)

 [E-mail to a friend](#)



[Tell O'Dwyer's what you think](#)

Commentaries on subject matter are welcome. Personal attacks are not allowed. O'Dwyer's reserves the right to cover any story it deems newsworthy.

Responses:

Brian Kilgore -- my photos love to be displayed in TJX frames (2/06):

Mr. Nicolazzo is one the right track, but one factor is missing, I believe -- an international perspective, but we in Canada are used to that.

First ... there's a question of just who is "selling" to the customer in the TJX situation. While the physical reallocation of the presence of the goods involved (you get the dress in the store) there are two business deals going on. When using a credit card, the dress-buyer enters into a business deal with the credit card company, not the retailer. The dress buyer owes money to the credit card company, not to the store. And the store has a relationship with the credit card company, not the retailer. Just follow the money. Dress buyer to credit card company to retailer. At what stage in this process does the dress retailer learn the name, address, telephone number, e-mail address, etc. of the person buying the dress?

So, how is TJX expected to call up the dress buyer, whose name is not known, whose address is not known, whose phone number is (probably) not known, etc.?

Seems to me this is the heart of the letter that should have been published in the paper, and posted on the store walls, the day after the breach was known.

And the first paragraph should have said, "We don't have a method, other than this ad, to tell our customers that your records may have been stolen. If you've done business with us, please call your credit card company and find out how it is protecting you."

And then the ad could go on to explain more of the situation. But get the safety instructions up top.

Up in Canada, the TJX mess affects two groups of customers. Some have bought at Winners and / or Homesense, two great chains, in Canada. And lots of Canadians have bought from TJX stores when visiting the USA. Up here, the ads were weeks late, too, and then the paragraph that matters was buried about two-thirds of the way down an ad created with no typographical skills.

Again, I'm thinking along Mr. Nicolazzo's lines. Was the ad deliberately designed to be hard to read, so few people would bother?

[Editorial Contacts](#) | [Order O'Dwyer Publications](#) | [Site Map](#)

Copyright © 1998-2007 J.R. O'Dwyer Company, Inc.
271 Madison Ave., #600, New York, NY 10016; Tel: 212/679-2471 or Toll Free: 866/395-7710