

## **en-terpret.co Case Study**

### **Sounding the Alarm: Using a Disclaimer to Raise Awareness of E-Mail Vulnerabilities**

#### **BACKGROUND**

Financial adviser John Shamash, of Ruby Stein Wagner in Montreal, faced a serious dilemma. His clients would regularly ask him to e-mail documents containing potentially sensitive information, but John knew the risks. Working with en-terpret.co, a Chicago-based international Information Technology and management consulting firm, John had taken an increasing interest in information security. He was especially troubled when en-terpret.co founder and CEO Daniel H. Harris explained how e-mail messages and attachments could be accessed by just about anyone in cyberspace as they bounced around from one server to another. John realized that his next “confidential” e-mail to a client might get more hits than the MSNBC Web site during a market meltdown. Although he had never lost a document, John was well aware of the potentially catastrophic consequences and wanted to find some way to better protect his clients and his own organization.

“I felt fairly comfortable with e-mailing if the client requested it,” John remembers, “although I always tried to be vigilant.”

#### **READ THE FINE PRINT**

Probably few people pay much attention to the disclaimers usually found at the bottom of e-mail messages. They are like the almost illegible user agreements that pop up in microscopic print when installing new software packages, or the litany of potential side effects that dominate pharmaceutical advertisements. Typically written by attorneys using impenetrable legalese, the disclaimers warn against forwarding the document without permission or otherwise misusing the information, especially if the reader is not the intended recipient. The disclaimers offer some

Phone: 773.868.4381

Fax: 773.913.6217

[www.en-terpret.com](http://www.en-terpret.com)

3642 N Magnolia, Suite 2

Chicago, Illinois 60613 USA

Associated Worldwide with JHI  
[www.jhi.com](http://www.jhi.com)



legal protection for the sender should the e-mail end up in the wrong hands, but as a deterrent to information theft or the careless transmission of vital data, their effect is practically nil.

Like other people, John had never given too much thought to the disclaimers. That changed one day when he received an e-mail from en-terpret.co. The disclaimer on that message, John says, “opened his eyes” and made him even more determined to raise awareness among his colleagues and clients about the potential dangers of e-mailing sensitive information. The en-terpret.co disclaimer read:

*Email as a communication tool is quite similar to a POSTCARD. Short, public and not certified in any way. As such, we cannot assure you that information you receive from us by Email is accurate, complete in every respect or even FROM whom you believe it to be from. In addition, as senders of Email, we cannot be certain that it is “You” (the “you” to whom this Email was addressed) that is reading this. Therefore, we offer NO ASSURANCE about the relevance or validity of information contained herein or the confidentiality and privacy of that information. We encourage you to TALK to us directly if you have any questions or comments.*

This disclaimer was much more powerful and effective than many of the others he had read, John says, because “It was like someone speaking directly to you.” John liked the image of a postcard; he felt it really helped to illustrate the nature of e-mail as an open forum. “Whenever I am composing an e-mail, I keep that in mind,” he says.

#### **CLEAR AND PRESENT DANGER**

After reading the en-terpret.co disclaimer, John was determined to make his own organization’s disclaimer just as strong and memorable. The intent was to not only





protect the firm, but also to alert his clients that their most critical data could be vulnerable. “Our main responsibility is to educate the clients,” John says.

As part of that process, John began to research e-mail disclaimers on the Internet. He located a number of relevant sites, mostly written by attorneys, suggesting specific wording to protect the sender in case the information is misdirected or misused. That was not enough for John. He wanted something that would get his clients’ attention and clearly state the potential dangers of e-mail, perhaps something like the warning on a cigarette package: *this could be hazardous to the health of your organization!* The en-terpret.co disclaimer seemed to be just the thing.

### **TAKING ACTION**

John says he is in the process of rewriting his firm’s e-mail disclaimer and will “definitely include” elements from the en-terpret.co disclaimer. Meanwhile, John and his colleagues have continued to work with en-terpret.co to bolster their own security protocols. The partners agreed that from now on, all financial data sent electronically would be password protected, although John knows that a password system is not infallible. For the most sensitive documents, John now creates an FTP (file transfer protocol) file, which offers an additional level of protection.

According to John, client response to the increased security measures at Ruby Stein Wagner has so far been muted, neither overwhelmingly positive nor decidedly negative. It is almost as if the clients have hardly noticed. “It is more cumbersome,” John acknowledges. “You cannot send someone a password by e-mail.” Although they might not realize it, however, John’s clients are much more secure thanks to his efforts.





### **LESSONS LEARNED**

John is quick to credit en-terpret.co for helping to shape his attitude toward information security while providing specific, practical steps he could take to protect himself, his firm and his clients. Rather than waiting for the inevitable information security crisis to happen, or burying his head in the sand and pretending that it could never happen to him, John was proactive. And en-terpret.co was there to help.

