

## BLACK TECH FORENSICS:

### New age technology threats and vulnerabilities

G. Stevenson Smith

#### E-Mail and Information Integrity

*ABC Corporation receives an e-mail confirmation on a customer order. The merchandise is shipped to the customer. Later the customer calls and says that the items were never ordered by their purchasing department.  
What went wrong?*

The use of information obtained from e-mail messages has reached the point where it serves as a key factor in influencing and affecting many business decisions. Consequently, it is important to have assurances about the integrity of such messages. Information does not have to be 100% accurate to have integrity, but upon receipt of the messages, we desire to know that the senders are who we think they are, and thus their representations are honestly made to us in good faith.

Unfortunately, e-mail provides an easy means of misrepresenting both the source of the message and the sender. Currently, most e-mail arrives without digital signatures which might help to provide stronger assurances of information integrity. As a result, e-mail messages have been a major contributing factor to the destruction of asset values around the world. Attachments to e-mail have at numerous times crippled corporate computer networks, as for example with the

Melissa and Love Bug viruses. The damage created by these two viruses alone was in the billions of dollars around the world. In addition, the misinformation about a company's financial prospects received as an e-mail message has contributed to a drop in stock prices that resulted in the disappearance of millions in market capitalization within a few hours, as occurred with the Emulex e-mail hoax.

In all these instances, information integrity within the e-mail has been purposely violated by the sender of the e-mail and corporate asset values have been diminished. Although there are methods that can be used to help prevent the occurrence of these activities beforehand, the purpose of this paper is to familiarize readers in understanding how the perpetrators of such activities can be electronically traced.

#### E-mail Headers and Tracing

In order to understand how perpetrators who send viruses and financial misinformation are traced, it is first necessary to understand some of the technical information found in e-mail headers. The header that we usually see in our e-mail is the short form of the header, and it shows the e-mail address of the sender and the recipient, the subject, date, and time. The time zone infor-

---

G. Stevenson Smith is Professor of Accounting at West Virginia University, Morgantown, WV USA.