SECURITY

Email Tampering—This Time, The Good Guys Won

Michael Weingarten and Adam Weingarten

Email is quick, it's convenient and it's used by just about everyone. But it can also be tampered with.

Remember the first time you found you had been hit by a computer virus? How about the first time your hard drive crashed and you hadn't backed up?

When things like those happen, you go through a process that starts with shock, moves quickly to rage, then to short-term damage control and, finally, to a resolve that this sort of thing will never happen to you again.

Our Signal Lake Venture Fund recently experienced a new type of threat: email tampering. We were sued by an individual who, among other things, said that he was owed warrants in one of our portfolio companies. We don't want to get into the details of the litigation or the equities of our position—other than to say that at the end of the day, the other side's case against us was thrown out in its entirety and the judge made a criminal referral for perjury. Sometimes, the good guys win.

From a *BCR* reader perspective, the litigation is interesting from two perspectives: ***a.***) To a large extent, much of the evidence trail came from email records; ***b***.) To bolster his case, the plaintiff took a real email sent to him by the CEO of one of our portfolio companies, and altered it to create a fake email containing damaging promises by our side. We were able to win by demonstrating that the plaintiff had tampered with evidence, perpetuated a fraud on the court and lied about the veracity of the email in an affidavit filed under penalty of perjury.

The net-net is to reinforce the growing role electronic communication plays in litigation and, as a result, that email evidence tampering is going to become increasingly common. As high-tech executives and managers of IT networks, it is incumbent on us to understand the risks associated with emails and to think about what we can do to protect our companies. We think a discussion of our case may prove informative.

What Happened To Us

Our saga began in February 2001. The fake email showed up in a court filing by the plaintiff, and was used as the centerpiece of his argument. In the quoted email, the CEO of one of our portfolio companies promised to give the plaintiff a large number of warrants as a consideration for fundraising activities, with no performance conditions attached. If unchallenged, this would undercut our position that the issuance of warrants should be based on achieving explicit performance guidelines, and our argument that since these were never met, no warrants were due.

As we read the plaintiff's pleading, we did not recall ever having seen the referenced email. We also believed that if the email had existed, it would have raised huge red flags during our internal litigation triage process; the whole thing smelled funny from the start.

Our immediate response was to check our fortunately complete email records for the day the message supposedly was sent. That showed that there was no email. Instead, however, we found that another email had been sent by the CEO to the plaintiff on the very same day and time of day (3:44 p.m.), *but on an entirely different topic*. Apparently, the plaintiff used the real email as a template, and used a text editor to change the message content.

As a further check, we looked to see if the alleged email showed up on any other day or time. Answer: no.

We then accessed the server log backup tapes maintained by our portfolio company. Since the email in question purportedly came from our portfolio company, for it to be real, it would have had to have gone through the company server.

Fortunately, our company maintained its own email server, rather than using a commercially hosted email service, so we could access records of all incoming and outgoing messages. Even more fortunately, the company's IT manager uses software that automatically makes a full tape backup every week, which is then sent to a third-party vault storage facility. Talk about good chain of evidence! When we accessed the server logs for the week in question, we found that the real email sent at 3:44 was there, the fake one was not. Obviously, if the disputed email was never sent, it could never be received.

As a further check, we hired the computer forensic group of a major accounting firm to confirm our beliefs. We realized that to charge the other side with computer fraud would be a "crossing the Rubicon" event, to say the least. Before we accused the plaintiff of anything publicly, we

Michael Weingarten (mikew @signallake.com) is a managing director of Signal Lake, a venture capital fund located in Boston MA and Westport CT. He also is managing director of Telecom Advisory Services at Monitor Group (Cambridge MA), a leading international strategy consulting firm. Adam Weingarten (adam@signallake.com) is a computer science student at Syracuse University, and Web master for Signal Lake.

wanted credible outsiders to investigate us as though we were the other side.

The forensics people proceeded to "mirror image" our hard drives. This is a process in which a forensic examiner uses special software to make an exact electronic duplicate of a hard drive, down to the bit and sector level. If you have a mirror image, it is virtually the same as having the hard drive itself, but without the danger of accidentally deleting information. Using the mirrored image, the forensic expert could look at all the visible files on the computer and see if the real and disputed emails were there. In addition, forensic examination of a mirrored drive allows one to look at the unused "slack space" on the drive (using special software), to see if there is any trace of the disputed email that is not ordinarily visible due to, for example, deletions.

In our case, the forensic group mirrored and then examined our hard drive data as well as the backup tape. The results supported our contention that the real undisputed email was sent to the plaintiff at 3:44 p.m., and there was no sign of the disputed email.

At this point, we went to court with our accusations. The plaintiff swore in an affidavit that we were wrong and the email was legitimate. Eventually, a court-appointed independent expert was hired to review the evidence from both sides and advise the court on the authenticity of the disputed email. One reason for doing this: Each side's hard drives contained privileged information (for example, emails to our respective attorneys). Only by having a court-appointed expert look at the original evidence could we avoid the privilege issues.

After some months, the independent expert issued his report and concluded that the disputed email was a fake. As it turned out, the issue wasn't even close. The plaintiff had taken the real 3:44 email and done text editing on it but, unfortunately for him, he was satisfied with making the visible email look real on the surface without realizing that there are lots of extended header fields that you don't always see, even if you select the "All Header" command on your browser.

As we learned from the forensics people, a full printout of the fake email header plus HTML information as extracted by a forensic recovery program ran for five pages. Apparently unaware of this, the plaintiff inadvertently copied three separate ESMTP server IDs from the real message onto the fake message, *without changing them.* Since these IDs are unique to a particular message, this was a dead giveaway that the message was a text-edited copy. Equally damning was the fact that the fake email had a creation date that was five months later than the supposed date of the email. There were also numerous other anomalies that we won't go into here.

At this point, the plaintiff's case unraveled and his claims were dismissed.

Reflections On The Case

From start to finish, it had taken us eight months from the point of identifying the email fraud to getting dismissal of the case. So, when the case went our way, we reacted with a combination of euphoria and relief.

We realized that in one important respect, we had lucked out; our opponent wasn't clever enough to do a sophisticated tampering job. Presumably, someone more technically capable could have changed all of the extended fields in a manner that would have appeared credible under initial forensic scrutiny, and that would have resulted in a much tougher fight.

So our longer-term reaction has been a realization that if we had protected ourselves better against email tampering from the start, maybe none of this would have occurred. In short, companies need to manage their email systems prophyllactically, because someday, those emails might become the center of legal fights.

After thinking about it, we have come up with the following advice and suggestions:

- **Emails Are Dangerous:** Be aware that when you send and receive emails, you are creating an important set of evidence that will be discoverable in the litigation process. A lot of people in telecom/high tech treat email as some sort of voice mail alternative. *WRONG!*

Voice mails typically get wiped shortly after they are received, particularly because most voice mail boxes have relatively modest storage capacity. Therefore, the evidentiary value of voice mails tends to be negligible.

By contrast, it's easy to keep emails on your hard drives indefinitely. And even if you don't keep your old emails, ***a.***) your opponent may, and ***b.***) computer forensic analysis could retrieve emails that you thought you wiped.

So, you really need to watch what you say on emails. Like pilots in a Tom Clancy novel, think "emission control." When you have a situation that potentially could go into conflict, stop sending messages by email. Instead, have live phone conversations.

- **You Need to Hold Onto Emails:** If emails are so dangerous, one potentially appealing option might be to wipe your drive periodically so as not to have discoverable evidence. You even could do a clean wipe, in which you overwrite your hard drive with 0's to totally foil any attempt to do a forensic recovery. This is consistent with normal legal practice, which is to get rid of records as soon as possible (and in advance of litigation) to minimize discovery production

On balance, however, we concluded that's not a good idea. First, if you are careful in what you say on emails, you needn't worry about discovery. Secondly, you need to assume that your opponent is carefully saving all of your emails, so your lack of documents won't work and may make you look as though you were trying to hide something.

More so than voice mail, email can become important evidence in litigation

You may have less ability to preserve email evidence if you use an outside hosting service

Conversely, if your opponent is wiping his/her drives and you have good records, you will have an advantage.

■ **You Need to Maintain Your Own Server and Keep Backup Logs:** Without question, the IT manager at our portfolio company who maintained such a meticulous server log backup system did us a tremendous service. Had the plaintiff done a better job of email tampering, the ability to prove that the message was never sent from our server would have been our most important piece of evidence.

From this experience, we have two pieces of advice. First, while it's easier and cheaper for small companies to host their domain names with ISPs, you lose the ability to keep server log records. It may be cheaper in the long run (particularly if you feel you have any legal exposure) to maintain your own email server—and an orderly backup process. Second, if you use an outside hosting service, pay the extra charge to get access to server log information and backup tapes. Then, send your backup tapes to a secure third-party vault facility. If your email size is modest, consider burning write once read many (WORM) CDs.

■ **You Need Digital IDs:** Shortly after the email tampering issue surfaced, we subscribed to a Verisign Digital ID. This is a relatively inexpensive encoding scheme that proves that you actually sent a particular email.

When you send out an email, the recipient (in Outlook and Netscape 4) sees a small tag on the upper right hand corner of the email that says "Signed." If the other party were to try to edit a real email sent from you, the "Signed" message would turn into "Invalid ID," which is a clear indication of tampering.

This has two benefits: First, it gives you an easy way to show that an ID is fake, without having to wait months for the final resolution. Even better, since any tampering is immediately discernable, your opponent, hopefully, will realize that the tampering won't work and not even try to falsify data. So, with a digital ID, you might just be able to discourage email fraud from ever happening in the first place.

■ **You Need Disclaimers on Your Digital IDs:** While we are fans of digital IDs, using them can create a potential problem if the recipient claims that the digital signatures are as legally binding as a signed agreement. From our perspective, we want to use emails (with some reasonable degree of caution) as a quick and painless form of communication. We don't want some plaintiff's attorney suggesting that an email intended as a casual conversation was, in fact, a binding contract.

To guard against this, we now include the following disclaimer on each email we send (it's easy to do this automatically as a footer in your browser program): "*The use of a digital signature by Signal Lake or any of its representatives is solely for the purpose of verifying the authenticity of e-mails sent by Signal Lake and its representatives and to prevent tampering with such e-mails. The use of a digital signature in this e-mail is not intended to create any binding contractual obligation on the part of Signal Lake or any of its representatives, and any such obligation must be evidenced by an agreement duly executed by the parties thereto on paper.*"

If someone wants a binding agreement from Signal Lake, they need to do it the old fashioned way—with signatures signed in pen. Check with your lawyer and consider something similar.

■ **If You Get An Independent Expert, Push For A Deadline:** In our opinion, it never should have taken our independent expert six months to come up with an answer. When we finally were in a position to see the extended headers of the fake email and compared it to the real one, we were able to pick out the duplications and inconsistencies within 30 minutes.

Why did it take the expert so long? We don't know, but we suspect that it had something to do with the fact that computer forensic examiners are overworked. In addition, since the expert worked for the judge rather than for us, we had virtually no leverage to push him along.

So, if you ever find yourself with a court-appointed independent expert, try very hard to get the Court to include some deadlines for delivery (i.e., mirroring of all drives to be completed by xx/xx/02, report to the Court and to the parties by yy/yy/02).

■ **Contextual Evidence Can Be Important:** If forensic evidence leads to a kill, that's great. However, if the criminal is technically proficient and your side hasn't protected yourself with email logs and digital IDs, you also need to consider contextual evidence—i.e. evidence that the disputed email makes no sense in the context of the evidence trail of the case.

In our litigation, we had several extremely strong contextual arguments in reserve, including, for example, evidence that the parties had agreed one month earlier to warrant compensation on a performance basis and with better terms for our side than in the fake email. Why would our CEO, with no intervening emails from the plaintiff expressing a need to change these terms, suddenly make unnecessary concessions?

Conclusion

Emails have become a central element of the business world, and are used as a casual element for communicating. In the process, however, they have become dangerous, a fact that isn't generally apparent until an email message is used against you or your firm. To defend yourself, think about what you need to spend to prepare in advance. Compared to the cost of litigation, the payback from investing in a well-managed email system can be huge□

Companies Mentioned In This Article
Verisign (www.verisign.com)