Logic Bombs (3):
Time Bombs in Contract & Commercial Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous two articles of this four-part series, we have looked at logic bombs installed by insiders and some basic principles for stopping them.

Today’s software is often provided by external suppliers. Individual contractors and small software firms continue to play an important role in creating systems especially designed to support the essential operations of countless organizations. Larger firms provide commercial off-the-shelf (COTS) software to millions of users.

In the movie Single White Female, the protagonist is a computer programmer who works in the fashion industry. She designs a new graphics program that helps designers visualize their new styles and sells it to a sleazy company owner who tries to seduce her. When she rejects his advances, he fires her without paying her final invoice. However, the programmer has left a time bomb which explodes shortly thereafter, wiping out all the owner's data. This is represented in the movie as an admirable act.

In online discussions, I have read communications from several consultants who brazenly admitted that they always leave secret time bombs in their software until they receive the final payment. They seemed to think that this strategy was a legitimate bargaining chip in their relationships with their customers.

In reality, such tricks can land software suppliers in court.

In 1988, a software firm contracted with an Oklahoma trucking firm to write them an application system. Some time later, the two parties disagreed over the quality of the work. The client withheld payment, demanding that certain bugs be fixed. The vendor threatened to detonate a logic bomb which had been implanted in the programs some time before the dispute unless the client paid its invoices. The client petitioned the court for an injunction to prevent the detonation and won its case on the following grounds:

- The bomb was a surprise--there was no prior agreement by the client to such a device.
- The potential damage to the client was far greater than the damage to the vendor.
- The client would probably win its case denying that it owed the vendor any additional payments.

I urge all programmers and contractors to stay away from these dishonest practices. More practically, I urge all clients of software contractors to be sure that their contracts explicitly bar any such mechanism for retaliation. The correct approach to avoiding this kind of fracas is to choose contractors with good reputations and to keep the lines of communication open at all times so that problems don’t escalate into warfare, covert or overt. It’s much better to pay lawyers to prevent lawsuits than it is to pay them to fight them.

In the last of these four articles, I’ll discuss renewable, time-limited licenses for commercial
software.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.