This article continues with newer methods of extortion that have popped up in recent years as the importance of cyberspace has increased to businesses worldwide.

Countless cases have been logged in which people have registered Internet domain names with significant commercial value (e.g., names of celebrities) before those people or companies have registered them. These cybersquatters then demand sometimes enormous payments to release the domain names. As a result of the trouble caused by legal battles over trademark violations, registration authorities set rules requiring registrants to be able to show the legal right to use the names they are registering. In recent years, many registrations made solely to extort money from trademark holders have been rescinded by the domain registrars. Some recent cases of cybersquatting:

* Musician John Tesh sued the owners of johntesh.com in January 2000, claiming that the only possible reason for the registration was to extort money for resale of the domain.

* In the two months after establishment of a cybersquatting arbitration service under the World Intellectual Property Organization (WIPO), 89 cases were registered. Early wins for trademark owners included the World Wrestling Federation, Stella D'oro Biscuit, and Telstra.


* A British company attempted to register domain names using the names of many authors; the Authors' Guild filed legal objections against the company in December 2000.

* Some companies specialize in monitoring expiration dates of domains with high profit potential and register them within seconds of their release by careless owners.

* The surprising frequency with which Web sites whose domains have changed hands have pornography posted on them may be the result of a deliberate strategy to increase the level of embarrassment of the former owners and a method for raising the price people are willing to pay to buy the lapsed registration back from the extortionists.

The most obscure form of extortion is sometimes called "patentmail." Companies who receive or buy patents on commonly-used high-technology principles or protocols sue victims with deep pockets for large sums. For example, one company has been "using a 1993 patent that covers a basic process for sending files between computers to demand license payments from big-name companies, including The Gap, Walgreen, Nike, Sony, Playboy Enterprises and Sunglass Hut. Other less-willing contributors include Audible, Encyclopaedia Britannica and Spiegel, which were threatened with litigation when they refused to pay up." [NewsScan, 2001-03-09]. Other patents cover such concepts as computer-based distance education and plug-and-play driver installation. The company has won $350 million in settlements so far.
How should one prevent victimization by extortionists? The most obvious measure is to enforce reasonable security given the sensitivity or criticality of one's data. Having adequate backups would be nice. Encrypting sensitive data so they cannot be misused even if the files are copied would also make sense for most organizations.

Second, be absolutely sure that you _never_ let your domain name lapse by accident. Even if you don't want to continue using your domain name, you should seriously considering paying the trivial sum required to maintain legal control over it so that bad people can't try to embarrass you with, ah, undesirable content.

As for avoiding blackmail, the only sensible response to attempted blackmail is the famous line, "Publish and be damned." Extortionists and blackmailers are by definition criminals; they're bad people and we cannot trust them. If someone is willing to break into a system or to abuse trust to acquire leverage of this kind, what possible grounds are there for supposing that they will stop once we give them what they ask for – at first? Police authorities are clear on the dangers of acceding to blackmail: it never stops. In espionage, getting an insider to commit a tiny peccadillo is the key to increasingly serious betrayal: at each step, the threat, implicit or explicit, is that the previous string of wrong-doing will be revealed.

As for patentmail, each case has to be decided on its merits. I just wish that more people would fight the broad claims of patent violation in court and thus increase the cost of doing business for these operators. In several cases, vigorous counterattacks have resulted in reconsideration of patents and judgement by the U.S. Patent Office that the patents were overly broad and thus invalid.

* * *

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.