CHICAGOLAWBULLETIN.COM Serving Chicago's legal community for 160 years WEDNESDAY, JANUARY 28, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 19

In an increasingly digital age, how can another Sony-style hack be avoided?

Investment in product development has always been a gamble. History is filled with stories of new products that were dismal failures, beginning with the Ford Edsel in 1957 up through "New" Coke in 1985 and, most recently, the Disney movie "John Carter" in 2012. Yet these well-known investment failures were largely due to misjudging consumer interest.

Today, new products face a new challenge to their investors — illegal hacks that place either the product itself or the trade secrets related to that product into the largely uncontrollable digital universe.

The hack of Sony's computer systems in late November resulted in the unauthorized release of embarrassing employee e-mails, personal records, the unpublished script for a new James Bond movie and copies of unreleased films. Even with the successful post-hack release of "The Interview" — the satire at the center of the controversy portraying an assassination attempt against Kim Jong Un — Sony reportedly still faces a $30 million loss for the film.

There is currently no foolproof technique for avoiding cyberattacks on products and companies. Even the Twitter page for U.S Central Command (CENTCOM) was hacked on Jan. 12. But there are steps intellectual property owners can take to reduce the impact such attacks can have on a company's product development.

Divide and conquer

Technology has made life so much easier. Product developers in different divisions can easily communicate with each other and share digital flowcharts, formulas and pre-release screeners in the wink of an eye. Anything that is in digital format can be hacked.

I am not advocating a return to face-to-face communications or paper-only distributions necessarily, although such techniques might be helpful for truly valuable information. Instead, projects need to be created with an eye to dividing the labor and keeping it divided as long as possible.

Research, development and commercialization aspects need to be separated. Digital walls have to be reinforced with constant reminders that employees should not send any information (in digital form or otherwise) except to those expressly authorized to receive it.

These old-fashioned steps are often overlooked in today's digital environment. Failure to stress and enforce distribution limitations in the current sharing culture only increases the odds that confidential information will be leaked.

Allowing employees to use unsecured equipment, whether at work or at home, similarly guarantees that any security measures a company takes will be circumvented. Strongly protected internal files become a hacker's fodder when an employees's children use that same computer to play a video game, watch a YouTube video or even chat with friends.

Encrypt critical information

Work-product and other confidential business information inevitably must be shared. Even if distribution is limited, which it should be, encryption remains key to protecting such information.

Encryption does not ensure that others will not be able to access the protected information. However, if such information qualifies for copyright protection, both the United States and other countries provide specific additional penalties for decrypting technological protection measures for copyrighted works.

Article 11 of the World Intellectual Property Organization Copyright Treaty expressly requires signatories to provide "adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors" to protect their rights.

U.S. law provides similar protection against circumvention of effective technological protection measures for copyrighted works. (17 U.S.C. Section 1201, et seq.) Penalties for the simple act of circumventing such protections can provide a basis for injunctive relief and criminal prosecution, without the need to deal with complex trade secret or fair-use issues.

GLOBAL IP

DORIS ESTELLE LONG

Doris Estelle Long is a law professor, director of the Center for Intellectual Property Law and chairwoman of the intellectual property, information technology and privacy group at The John Marshall Law School. She has served as a consultant on IPR issues for diverse U.S. and foreign government agencies, including as attorney adviser in the Office of Legislative and International Affairs of the USPTO. She can be reached at 7long@jmls.edu.

Films, such as "The Interview," are plainly copyrightable. But compiled fact works such as research reports, marketing proposals and charts and graphs also qualify. No research on critical product development should be allowed to circulate without such encryption.

Not all security is created equal

Although each hack of a Twitter feed, a website or a company's computer system receives media attention, not all such attacks raise the same level of concerns.

The recent hack of the CENTCOM Twitter site was undoubtedly problematic from a public relations point of view, but Twitter feeds have notoriously low, or even nonexistent, security. Such a hack did not represent a threat to sensitive records. By contrast, hacks of internal company computers or servers, such as occurred with Sony, guarantee that confidential information is being compromised.

Given the variable levels of security that exist in different digital venues, companies should carefully audit what types of access it allows to internal records, including express instructions regarding what items should be shared on Twitter and other social media sites. More significantly, security features for internal development records should be high. As more inventors store lab and other development records in digital format, the ability to lose critical trade secret protection increases.

Both domestically and internationally, confidential information must subject to "reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret." (TRIPS, Article 39. See also 765 ILCS 1065/2(d)).

In *U.S. v. Du*, the 6th U.S. Circuit Court of Appeals last year found that the use of multiple passwords for individually higher ranked files — one for network access, one for access to individual folders, culminating in files available only with a manager's password — helped demonstrate sufficient reasonable steps to protect General Motors' plans for its hybrid engine.

This step-by-step approach does not guarantee that no "disgruntled former employee" will ever disclose a company's confidential information. But it ensures the ability to secure injunctive, and other, relief if such disclosure occurs.

Think outside the box

The Sony hack has been used to resurrect failed digital enforcement measures, including the U.S. Stop Online Piracy Act and the multi-lateral Anti-Counterfeiting Trade Agreement. Both of these attempted to deal with the problem of digital piracy and counterfeiting through measures that were deemed either too heavy-handed or ill-advised.

There is no question that more effective enforcement is required. Instead of falling back on past techniques, we need to focus on new multi-national enforcement standards that combine intellectual property enforcement with the precise harms caused by cyberattacks.