CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

TUESDAY, MARCH 3, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 42

# Cyberspy thriller with an unclear ending

It reads more like a spy thriller than a news story. Employees of the U.S. subsidiary of a global technology and media company log on to their computers one Monday morning and are greeted with the menacing figure of a neon red skeleton, announcing that the company has been hacked and threatening the release of massive amounts of confidential data unless certain unspecified demands are met.

Over the next few weeks, while the company ascertains how much and what kind of data may have been stolen — and races to secure its systems — the hackers release enormous amounts of information pilfered from company networks. The company faces a media firestorm as confidential, and at times embarrassing, information is revealed about its projects, finances and internal workings.

The situation only worsens when the company cancels the release of a motion picture satire about a plot to kill North Korean dictator Kim Jong Un after the hackers — who call themselves the Guardians of Peace — threaten "September 11 type" attacks on theaters that show the film and national theater chains cancel their premieres. When the company reverses course and agrees to release the film, critics suggest it was all a publicity stunt. Meanwhile, an international incident is brewing as U.S. officials point at North Korea for the hacks.

In the movies, the good guys would capture the bad guys, and the world would be a safer place for moviegoers and corporations alike.

But the bigger question is, What happens in real life?

Cybersecurity is not a new topic. A steady stream of data breaches has been reported over the last several years. The Sony Pictures breach was far more limited in scope, yet it made a bigger splash with its celebrities and dictators. It also provided lawmakers and the White House with a sensational reason to reinvigorate the cybersecurity debate.

President Barack Obama used the situation to renew his call for bipartisan support for cybersecurity protections.

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families, especially our kids," the president proclaimed in his State of Union address. "If we don't act, we'll leave our nation and our economy vulnerable," Obama continued. "If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe."

Rhetoric notwithstanding, the White House cybersecurity agenda hasn't changed dramatically from previous years, calling for two measures that would directly affect companies in anticipating and responding to data breaches: a notification law and cybersecurity information sharing between the private sector and Department of Homeland Security.

Members of Congress seem not to disagree on the need for a data breach law, which would replace the patchwork of 47 state laws currently in place. Even so, numerous bills have been introduced — five in the Senate last year alone — but none has progressed very far.

In an attempt to jump-start the legislation, a House subcommittee began hearings recently to answer several questions:

• Which industries and entities should be covered (and should medical and financial interests be separate)?

PRIVACY, TECHNOLOGY AND LAW

**Nerissa Coyle McGinn**

*Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law as well as intellectual property law, focusing on trademark clearance and counseling.*

• Should a federal law take the place of or pre-empt state laws, and what role should state attorneys general play?

• What might the regulatory scheme for breach notifications look like, and what types of breaches would be covered?

• How long would companies have to investigate breaches before notifying consumers and what happens with notification violations?

Obama advanced his own proposal for regulations governing data breach notifications, which would pre-empt state law.

While the Personal Data Notification and Protection Act is similar to previous bills, it does present a few potentially controversial differences, including covering a larger category of personal information, the release of which alone would constitute a data breach. (Many other bills consider the exposure of information such as driver's license or passport numbers to be a breach requiring notification only when disclosed along with individuals' names).

The White House proposal also exempts breaches posing no reasonable risk of harm that individuals' data was compromised. The data breach law also would exclude small businesses that do not process large amounts of personal information.

The White House's second major provision involves information sharing between the government and private sector to help identify threats before breaches occur. The topic has proved particularly divisive in the past, in particular over liability protections for businesses.

Consumer privacy advocates also have raised concerns that information sharing, particularly when companies are protected from liability, would result in private entities turning over greater quantities of personal data to the government while allowing the government to use this information beyond its intended (and theoretically limited) purpose of cybersecurity.

Congressional hearings have started on the information-sharing bill, with a number of prominent business groups, including the U.S. Chamber of Commerce and the American Bankers Association, urging Congress to pass a bill as long as it contains appropriate protections and limitations. Meanwhile, in early February, the administration announced the creation of the Cyber Threat and Intelligence Integration Center to amass cyberthreat data gathered by different agencies and share it across the public sector.

While the truth-is-stranger-than-fiction Sony hack likely will remain in the collective memory of the American public for some time, the end of the story remains to be written by Congress and the Obama administration.