Bloomberg BNA

Big Law Business

LEGAL COMMUNITIES

A Business of Law Community

Coming Unwired: Time to Reconsider How We Deliver Market Moving News

August 14, 2015

Editor's Note: This post was written by a practice leader at law firm Patterson Belknap Webb & Tyler LLP.

By Craig A. Newman, Chair of the Privacy and Data Security Practice, Patterson Belknap Webb & Tyler LLP

It was the ultimate digital heist.

Cybercriminals from the Ukraine and rogue traders and small securities firms from Moscow, Paris and Malta banded together **to hack into the servers of three financial wire services** to steal market-moving information before it was released to the investing public. By then trading on this inside information, the criminals reportedly netted themselves more that $100 million in illegal profits. The two federal indictments and a companion Securities Exchange Commission case read more like cyber spy novels than legal complaints. They also beg broader, more

fundamental questions of governance that companies will need to sort out sooner, rather than later.

Caught up in the midst of this global fraud are Business Wire, PR Newswire, and Market Wired, favored tools of public companies to release their earnings reports, merger activities or other market moving news. Wire services have always been considered transparent, reliable and highly effective. Or so we thought.

But with these wire services now in the crosshairs of hackers and a global insider trading case, it's time to rethink how market moving news and information is disseminated, particularly in a digital environment where communications are immediate and the threat of cyber-attacks have never been higher.

The scheme itself provides insight into the vulnerability of a time-tested process, and the need to consider change. It was all relatively straightforward and repeated 1,000 times during a 5-year period. For the dozens of public companies involved, it was business as usual. They would send their draft earnings releases, changes in financial guidance or other "material" disclosures to one of the three wire services. The press releases were then uploaded to a server until it was time for public release. But between the time the press releases were uploaded and released to the public, a "window of opportunity" opened, during which federal authorities charge hackers stole copies of the releases and used the information for illegal trades. The "window" varied from a few days to just minutes.

While the $100 million the hackers are alleged to have made during their venture is certainly eye-catching, this isn't the first time a wire service has been hacked. In 2005, the U.S. Securities and Exchange Commission also charged traders from Estonia with hacking into Business Wire to steal news before it became public.

In theory, it should come as no surprise that third-party vendors like wire services are vulnerable to hacking. But as this week's indictments show, we are quickly approaching a train wreck when it comes to data security and the integrity of our public markets. If maintaining a level playing field remains the goal – where all investors have access to the same information at the same time – now is the time to begin asking the question: is there a better and more secure way of disseminating market moving information?

Should companies be releasing earnings or other material developments themselves on their websites, or through an SEC filing that bypasses the wire services altogether? What safeguards can be put in place to minimize the chances of this happening again? Would encryption technology have stymied the hackers? And why are news releases containing material, non-public information sent to wire services days or even hours before release, and then uploaded to sit on servers that are vulnerable to cyberattack?

These are just a few of the fundamental questions that corporate leaders should be asking themselves and their boards. With so much at stake, this isn't the time for corporate leaders to sit on the sidelines. The risks to the markets and their shareholders are far too great.