Major U.S. law firms have become more vigilant in recent years about the risks of cyberattacks, but revelations this week of a major hack on two New York firms are a reminder that the industry remains vulnerable.

The Manhattan U.S. attorney's office unsealed a criminal indictment Tuesday against three Chinese men accused of using stolen law-firm employee credentials to access troves of internal emails at two law firms. The men, according to prosecutors, used details they obtained in law-firm partner emails about pending deals to make more than $4 million in illegal stock trades.

While the indictment didn’t name the firms, The Wall Street Journal previously reported that prosecutors were investigating a hack at Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP. Details in Tuesday’s indictment indicate those two were the firms in question.

Spokeswomen for the firms declined to comment Wednesday.

Manhattan U.S. Attorney Preet Bharara said the case should serve as a reminder to law firms that “you are and will be targets of cyber hacking, because you have information valuable to would-be criminals.”
Legal-industry experts say law firms often lag behind their corporate clients in data-security measures, even though they are entrusted with valuable trade secrets, market-moving deal news and other sensitive information that is attractive to hackers.

The reason behind the gap is twofold: Lawyers have only felt the threat recently, and law firms traditionally lag behind other industries in trying to become more efficient through technology, largely because they bill their services based on time.

“Law firms aren’t necessarily committed to things that don’t make them money per se,” said Neil Watkins, the senior vice president of security, risk, compliance and privacy at legal-services company Epiq Systems. Mr. Watkins said law firms are at least three years behind what’s become standard for data security in finance and other industries, though he says awareness is improving.

Starting a few years ago, large banks began requiring their top law firms to undergo data-security audits and meet stringent standards.

That level of scrutiny is now being applied by other sectors. Marsh & McLennan Companies Inc.’s general counsel, Peter Beshar, said that in recent months, he’s begun requiring his top 10 outside law firms to meet six cybersecurity standards, including using encrypted transmissions when sending messages externally, having detailed incident-response plans and securing $5 million in cybersecurity insurance coverage.

To help stay ahead of a breach, law firms have formed an information-sharing group to learn about new potential threats and system weaknesses from both each other and government agencies. The group, which so far counts more than 100 firms, helped disseminate information on a potential threat a few months ago and thwart a hack, said Bill Nelson, chief executive officer of the Financial Services Information Sharing and Analysis Center, which oversees the legal group and similar entities that focus on other industries.

“It was a big wake-up call for many law firms,” Mr. Nelson said.

Los Angeles family-law lawyer Stacy Phillips said the need to protect the personal information of her clients was at the top of her mind earlier this year when she merged her boutique law firm into Blank Rome LLP, a 600-lawyer firm based in Philadelphia. Investing in adequate data-security technology was becoming “prohibitively expensive” at the smaller firm, she said.

“It was very much a stress,” she added.

Now at Blank Rome, she said the matrimonial practice, which holds extremely private information from client divorces and custody battles, has a double layer of security to ensure no one else at the firm can access their files.

At 650-lawyer firm Nixon Peabody, chairman Andrew Glincher said the firm is constantly looking for ways to improve its security, which at times has meant recognizing that some data is better protected by storing it with cloud-based vendors. The firm sends out mock phishing emails to raise awareness among employees and has invested in new technology and outside monitoring services to help with intrusion detection, data leakage, email filtering and virus protection.

So far, law firms have faced few financial repercussions for weak security systems. Chicago attorney Jay Edelson, who specializes in data-privacy litigation, would like to change that.

Over the past two years he’s investigated law firms for having potentially weak security systems, and filed lawsuits against firms for having inadequate data security. So far, just one of the suits has become public, with the rest filed under seal.

That public case, against trial law firm Johnson & Bell Ltd., doesn’t claim that any data was stolen, but instead that the firm had security holes in its time-entry system, email system and virtual private network. The case is now in arbitration.

Johnson & Bell co-founder and President William Johnson said in a statement that the firm will defend itself against the “baseless” lawsuit and that, “Our data systems are secure and our clients’ information is protected.”

Write to Sara Randazzo at sara.randazzo@wsj.com