http://www.terralex.org/publication/pa55d6c9cb1

In late December 2016, the United States Attorney's office in Manhattan unsealed an indictment accusing three Chinese traders of hacking into two US-based global law firms to obtain insider information on mergers and acquisitions activity that they later exploited to gain more than US$ 4 million in illegal profits.

For lawyers and firms, it's a chilling reminder of the challenges they face protecting not only their own data, but that of clients. And a potentially costly one: while the law firms that were victims of the hack have not been charged with wrongdoing, it may not be long before authorities around the world begin to stop treating law firms as "victims" of hacks and start considering them responsible parties who have not done enough to safeguard the confidential information of their clients. Not to mention the impact on a firm's reputation (and revenue stream) when they have to alert clients to the hack…

So what can lawyers and firms do to make it more difficult for hackers to get in the door? Here are three steps you can take today:

1. **Impose a strict password policy**. US authorities say the traders accessed the victims' servers more than 100,000 times over what appears to be at least a 12-month period, downloading millions of documents from the law firms' servers (including more than 40 gigabytes of data between August 1 and August 9, 2014). Did the law firms require password changes during that time? Maybe. But the hackers' continued access to confidential emails suggests that they were able to return time and time again to the same email database during the entire operation, using the same stolen password(s). Of course, there's no guarantee that a password change would have stopped them, but at the least it would have made it harder for them to steal client data. Requiring all users of the firm's email server to change their respective password several times each year should be seen as a first and minimum step. A second step could be that the firm's password policy imposes a minimum password length and complexity (using both upper-case and lower-case letters, special characters and numerical digits), and rejects any blacklisted passwords. Using a password blacklist is necessary to prevent users from choosing passwords that are deemed insecure. In a best case scenario, the firm would not let the users create their respective password, but rather create it for them (using a random password generator), which would prevent situations where the password created by a given user is identical to the one he/she uses to access his private email account or any kind of online services (such as online bank accounts, social networks, etc.).

2. **Train your employees**. No mention is made in the indictment of how the hackers were able to obtain IDs and passwords of employees at the two victim firms. But it's not a stretch to assume that they convinced the employees themselves to voluntarily give up that information through "phishing" attacks, where hackers use legitimate-looking emails to convince users to share a broad range of information, from passwords to banking details to other sensitive data. Teaching everyone in your firm with an email account – from the mailroom staff all the way up to the Managing Partner – to avoid clicking unknown links and report suspicious emails can stop hackers before they get in the door. Your employees need to be aware of the existing risks. They need to understand that a hacker may rely on their everyday use of the internet to track and identify a "hole" which may be used. They should be encouraged to regularly modify the passwords they use on their everyday digital life. More than this, attorneys need to recognize that they represent their clients' first – and sometimes only – line of defense when it comes to highly confidential information. Telling a lawyer that they need to change a password because it is good data hygiene is one thing; telling a lawyer that they must be tech savvy and aware of data security risks as a component of their professional responsibility to their client is another.

3. **Update and secure your systems**. It would appear that the accused traders were successful because they were able to install malware on the servers of the victim firms. Given they were able to accomplish this, as described above, is probably more of a training issue than a technology one. But once that happens, once the malware is actually up and running, data security must take over, to find and eradicate the virus lurking on your server. Although it goes without saying, every single machine used by lawyers and staff must utilize the most up-to-date protection software for your systems. This latest incident suggests that even sophisticated global firms could use a tighter set of policies and procedures for protecting their data. Firms should prioritze the security of their IT systems (servers, computers, LAN networks, wifi, webcams, etc.), but also of the mobile devices which are used by the employees in their professional practice. In this regard, BYOD ("bring your own device") policies should be avoided if possible, as they certainly increase security breach risks. Control of access to information is also a critical component of data safety. By limiting the number of people with access to materials (e.g., restriction of access to a matter to timekeepers for that matter, or requiring billing-partner approval for review of highly confidential documents) vastly limits the possibility of a breach. Fewer access points means fewer occasions for a hack.

* * *

But it's not all bad news: according to the indictment, seven other law firms targeted by the hackers were able to withstand the attacks, including one firm that held off more than 5,000 infiltration attempts over a three-day period in 2015. Isn't that the firm that you'd like to be?

Co-Authored by:

James J. Ward, Lance Godard, Benjamin Jacob