Published on *The National Law Review* https://natlawreview.com

Spearphishermen Catch Big Fish re: Data Breaches and Securities Fraud

Article By:

Amy R. Worley

Data security is too often synonymous with the loss of consumer financial information. A recent report by a cybersecurity research firm reminds us, however, that a data breach can have an impact far beyond consumer privacy concerns. On December 1, 2014, FireEye Inc**. announced that a group called "FIN4" was duping** executives, lawyers, and financial consultants into providing access to **confidential and proprietary information at publically traded companies**, and that FIN4 was using that information to gain an advantage in the stock market. In other words, FIN4 was using data breaches to commit securities fraud on a massive scale.

This scheme reminds us that data breaches can be a vehicle to commit analog crimes. The FireEye report describes hackers using authentic Securities and Exchange Commission documents to deceive (presumably seasoned) finance sector workers into revealing their authentication information (username/password) to the fraudsters. Schemes like this one, that do not rely on hacking but, instead, trick users into disclosing passwords, are known as "spearphishing." The term intentionally invokes images of a sportsman patiently waiting to catch a specific fish and stabbing it with a long spear, rather than casting a wide net and catching any fish that unwittingly swims into it.

FireEye believes that there may have been spearphishing attacks at as many as 100 publically traded U.S. companies. This means that for the affected companies, there may be fraudsters with prying eyes still inside their networks—operating on authentic credentials—following inside communications about revenues, costs, potential mergers and acquisitions—all things that move markets.

There are several lessons still to be learned from the FIN4 scheme, as the researchers continue to uncover its breadth. That said a few morals to this story are apparent. First, there are scarier fish in the sea than just malware and zombie bots. Companies simply must train employees how to recognize and respond to spearphishing and social engineering attacks—hackers use psychology as often as they use malicious code. There should almost never be an occasion that an employee must provide anyone else at his or her company with a password. Most business software provides an automatic password reset function using shared secret technology that sends an email to the user allowing him or her to reset forgotten passwords.

Second, this is the type of attack that a good cyber security and data privacy risk assessment can

often spot and prevent. If your company doesn't have technical systems in place that prevent employees from ever needing to share passwords with IT or management, then your company could fall prey to an attack like this. A good risk cybersecurity and data privacy risk assessment can spot this and other types of spearsphishing and social engineering risks and help your company eliminate them before they are exploited.

Finally, company business information must be protected as thoroughly as customer data. This requires, among other things, a good data classification system. If your data is properly classified as confidential then your information technologists can segregate and protect it much better from attacks.

Hackers know their targets. Does your business know your hackers?

National Law Review, Volume IV, Number 338