Is your company's share price safe?

Closed-loop authentication security alert for public company websites and IR websites

Any IR professional's biggest nightmare is to see your company's stock crash. Also on the nightmare list is trading being halted and the unforgiving media attack surrounding a security breach that could have been prevented. If it turns out to be caused by your action or inaction, it could be career ending. To avoid this type of catastrophe, it is essential to ensure that key vendors have appropriate controls in place to prevent inaccurate information from being published on behalf of your company.

Lucent Technologies, Emulex Corp, Bid.com, and PairGain Technologies are just a few companies whose stocks suffered in the past due to the publication of fake press releases, causing their stock prices to drop as much as 60-70%. Since these incidents, newswire vendors are aware of how unsecure email is and have changed their policies and no longer accept press releases from clients via email. However, press releases are not the only avenue for publishing market-moving information. Automated bots from Bloomberg and other companies constantly scour public companies' websites for updates that could affect the share price. An unauthorized update could have a devastating impact within minutes.

If your website or IR website vendor accepts change requests via email, you have a security problem and your company may be at risk.

One aspect of email that many people are not aware of is the ability to "spoof" an email, or send an email that appears to come from another person. Email software relies on the honesty of the sender when displaying the from address that an email was sent from. As a result it is very easy to send a fake email from any email address to any person or company. It is difficult, even for an experienced technical person, to determine whether the email is authentic. Email spoofing is readily available to anyone with an Internet connection, as indicated by the 1.6 million Google search results for "email spoofing service."

If you can request updates to your website, changes in user access, or other any other changes, your provider needs to be using closed-loop authentication. Closed-loop authentication is a way of verifying the authenticity of an email request before any action is taken. Here is how authentication works - when you email a request for an update/ change in, the vendor sends an email to the authorized users email address on file, which includes a security code. Once you click a link in that email or send back a reply including the security code, the request is considered authentic. This ensures that the person sending the email can receive email at the address as well as send email from it. Of course they also need to ensure that the sender is an authorized user, permitted to make the changes in the first place.

You may be surprised to learn that we only know of one website and IR website provider serving public companies using closed-loop authentication.

Equisolve provides fast, efficient, and most importantly, **secure technology solutions** to hundreds of public companies.

If you'd like to learn more about how you can protect your business and investors, contact Equisolve's CEO Tom Runzo or visit www.equisolve.com.