2-ZDNet-Breach

Log Out

Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades

LinkedIn executives reveal on quarterly earnings call just what the June theft of 6.5 million passwords cost the company in forensic work and on-going security updates.

John Fontana Contributor

John Fontana is a journalist focusing on access control, identity, privacy and security issues. Currently, he is the Identity Evangelist for strong authentication vendor Yubico, where he writes and edits a blog, as well as, directs several social media channels and represents Yubico at the FIDO Alliance.

Posted in Identity Matters on

August 3, 2012

| Topic: Security

LinkedIn spent nearly $1 million investigating and unraveling the theft of 6.5 million passwords in June and plans to spend up to $3 million more updating security on its social networking site. *[Rebuild]*

During Thursday's second-quarter earnings call, which was otherwise rosy with revenue up 89% to a record $228 million, Steve Sordello, LinkedIn's CFO, said forensic work on the password theft was "roughly $500,000 to $1 million."

Sordello said the company plans to spend between $2 million and $3 million on security upgrades post breach. *[Rebuild]*

LinkedIn CEO Jeff Weiner didn't dwell on the breach, treating it as just another bullet point in his report to Wall Street. *[Diminish]*

"Part of adding value to our members every day means ensuring that their experience on LinkedIn is safe and secure," he said. "Since [the breach], we have redoubled our efforts to ensure the safety of member account on LinkedIn by further improving password strengthening measures and enhancing the security of our infrastructure and data. The health of our network as measured by number of growth and engagement remains as strong as it was prior to the incident." *[Rebuild]*

In June, LinkedIn reported that Russian hackers stole nearly 6.5 million passwords. Users, who are prone to reuse passwords across different web sites, were urged to change their passwords. With more than 160 million users (at the time), the password theft involved less than 5% of LinkedIn's user base.

The hack, however, was embarrassing given that LinkedIn was victim of a common SQL injection attack. *[Disappointment]* In addition, it failed to comply with basic industry standards by using a weak encryption format, and neglected to "salt" the encryption hash, which weakened security .

The breach doesn't seem to have slowed down LinkedIn's business, it reported cumulative membership growth of 50% year-over-year and now has 174 million members *[Positive]*. The company reported it is adding approximately two member signups per second.

In addition, 75,000 third-party developers now use LinkedIn's APIs to build innovative services off of LinkedIn, an increase of 15,000 since February.

The transcript of the LinkedIn earnings call is available at www.seekingalpha.com .

See also: