AP

Monster Breach Teaches Familiar Lessons

Friday August 31, 2:31 pm ET

By Brian Bergstein, AP Technology Writer

Monster's Data Breach, Subsequent Security Efforts Highlight Uneven Online Practices

By now, the perils of securing online data with little more than user names and passwords should be well known. Monster.com learned that lesson late and the hard way, prompting this week's announcement that the Web jobs board will spend millions of dollars to improve its security.

Monster Worldwide Inc. recently discovered that con artists had grabbed contact information from resumes for 1.3 million people -- and likely many more, since Monster now says this was not an isolated incident. Files were pilfered not only from Monster.com but from USAJobs.gov, the federal-government career-listing service operated by Monster.

The stolen information is not by itself ultra-sensitive, since resumes generally do not include Social Security numbers, financial data or account information.

But contact information alone can be lucrative for online criminals, who used what they got from Monster to craft "phishing" e-mails that go after such sensitive data.

The affair could serve as a warning to other businesses that operate online. But if the past is any guide, many will shrug off this episode.

"You're going to see this happen again and again and again," said security analyst Bruce Schneier, chief technologist for BT Counterpane. "I assure you, every other company didn't say, `Wow, look what happened to Monster, we have to fix our problem.'"

Blame many factors. For one, upgrading security can be expensive, and many companies are reluctant to shell out for improvements until they've been viscerally reminded of the need for it.

"How do you justify a $10 million security budget when nothing happened last year?" said Mark Rasch, a former federal cybercrime investigator now with FTI Consulting Inc.

Another problem is that companies are hesitant to put up blockades that can annoy legitimate users.

"We're all accustomed to a straightforward and easy experience," said Dennis Maicon, executive vice president of Digital Resolve, a unit of Landmark Communications Inc. that sells automated fraud-detection systems. "We want to do things quick, we don't want to jump through all kinds of hoops to say, `Hey, it's me,' because a good portion of the time, it is you. A company like Monster has to maintain the customer experience."

That balance can shift, of course, if regulations require more stringent security. Many financial institutions and insurance companies have adopted extra measures like Digital Resolve's authentication technology as a result. It lets customers sign on in a straightforward way but scans for anomalies (the user is signing on from, say, Romania all of a sudden) that might indicate an unauthorized person has stolen the password.

After the Monster breach was disclosed by researchers at Symantec Corp., Monster defended its policies by pointing out

that its network security had not been broken. No one hacked in, after all. Rather, the criminals obtained legitimate keys to the system -- most likely by phishing or guessing passwords belonging to recruiters with access to Monster's tens of millions of resumes.

Yet the chance that someone would co-opt legitimate access to a network should itself have been considered a security flaw.

In one of the most infamous incidents, data-gathering giant ChoicePoint Inc. found in 2004 that criminals had posed as honest-to-goodness customers and filched information on 163,000 people. ChoicePoint ended up spending about $30 million fixing the situation, including $15 million to settle charges from the Federal Trade Commission that its standards were weak.

It's unclear how much of a hit Monster's breach will cause the company, which already has been struggling. A month ago it announced layoffs of 15 percent of its work force. The stock is near 52-week lows and a key finance executive just departed.

To respond, Monster has said it would spend at least $80 million on upgrades to its site, which now include security changes.

The company described those steps in general terms this week after realizing that its data had been probed more than once. Among the tweaks will be closer monitoring of the site and limits on the way its data can be accessed.

Some of those practices might already be in place at rival online job boards. For instance, both CareerBuilder.com, which is owned by newspaper companies and Microsoft Corp., and Yahoo Inc.'s HotJobs say they limit the number of resumes that one user account can access over a given period. (That is of limited effect, however, if fraudsters corrupt multiple accounts, which is a common pattern.)

CareerBuilder spokeswoman Jenny Sullivan added that her site has software that monitors for excessive or otherwise unusual usage patterns. Last week, CareerBuilder began "scrubbing" Social Security numbers and other sensitive information out of postings left by job seekers, though Sullivan said that step was in the works even before Monster's breach.

The unavoidable truth about computer security, though, is that such steps can slow but not stop online fraud. Gartner Inc. security analyst Avivah Litan advises job-seekers to use a separate e-mail account for career queries and publicly post only basic contact information, nothing more than what could be found in the phone book.

"Assume nothing's safe," she said.

Monster.com's security page for users:

http://help.monster.com/besafe