The Uber breach: What matters most!

December 13, 2017

When hackers accessed the personal information of 57 million riders and drivers—media outlets went wild. Everyone was taking about how Uber covered up the hack. And over here at RightSize Solutions, all we could think was: Really?! That’s what you’re paying attention to?

Yes, Uber tried to sweep the breach under the rug. Yes, this is outrageous—but the focus on the cover up has detracted from the scariest part of this story.

Here’s what should really be shaking the world about this breach:

The breach began when the attackers accessed the information on GitHub.

GitHub is a site where software engineers and developers share code (often when more than one programmer is working on the same project)—and in this case, one of the developers of Uber left the login credentials for the Amazon Web Services account which housed the personal details that were accessed.

It was that simple. A developer left login information somewhere. It was found by hackers. And it was used to perpetrate a massive breach.

We were glad to see this angle addressed by Bloomberg Technology: Uber Hack Shows Vulnerability of Software Code-Sharing Services, which notes, “Hackers hunting for vulnerabilities routinely scan code posted publicly to Github for passwords and private encryption keys that developers have left visible.”

So even if your website is up…

Even if it’s running smoothly…

Even if it’s completely secure…

You have to ask the question: What happened before all that?

Who made the site? Are login credentials floating around somewhere online? Has private information been shared during the development process—by accident or on purpose—that you don’t even know about?

The real issue isn’t that Uber got hacked.

Or that they covered it up.

It’s this: Where was management to maintain security during the development process?

At RSS, we will keep your information secure every step of the way. Let’s talk about how.