Verizon data leak amplifies importance of third-party vendor risk management

| Thursday, July 13, 2017

Ever heard of NICE Systems? No? Well, there's a good chance they've heard about you and have been keeping records on your data. NICE Systems serves 85 of the Fortune 100 as customers and provides recording services for customer service calls, among other things. They count Verizon as one of their customers and just leaked the personal data of over 6 million Verizon customers through a simple misconfiguration on one of their hosted sites.

NICE Systems is one of countless third-party vendors that process personal information for the businesses that we interact with everyday and never hear about. There is nothing new about this, or even this type of breach. In fact, most large breaches are the result of a breach of a third-party vendor.

So, what is there to do about it?

Most of the large organizations that we interact with every day have third-party risk management groups that are responsible for ensuring that these third parties have adequate security measures in place before the large organization agrees to allow its customers' personal information to be processed by the third party. These third-party risk management groups will generally revisit their assessments of the third parties on some sort of a recurring basis to make sure that the third party is still keeping adequate security measures in place.

This system is broken. Most third-party risk management groups rely solely on self-attestation questionnaires filled out by the third party with no verification that any of the security measures that the

third party claims to have are actually in place and active. Even in those instances where a third-party risk management group engages in more robust investigations, including verification of audits, inspection of policies, and even conducting their own on-site assessments, these are only conducted on an every-so-often basis, generally once every one to three years. A lot can change in that amount of time, exposing an organization's data entrusted to the third party to unassessed risk.

All the details of exactly what happened with the Verizon breach are not available yet, but what is generally known is that the misconfiguration that caused over 6 million customers' data to be exposed could have been easily discovered through an adequate assessment of the hosted site's account settings. The problem is that third-party risk management programs rarely, if ever, require regular assessments and reports of technical controls by their third parties and almost never actually verify the controls, instead relying on the third party to verify them themselves. The result is 6 million records being needlessly exposed.

These types of breaches will continue to occur until third-party risk management programs adapt and begin to require the same level of diligence by their critical third parties as they would require of their own organization. There exist today several solutions that can give organizations real-time visibility into the actual technical controls of their vendors and these solutions make the typical assessment process much faster. It's time for organizations to rethink their third-party risk management programs and look into leveraging new technologies, contractual provisions, and other tools to get a better picture of how their data is actually being protected.