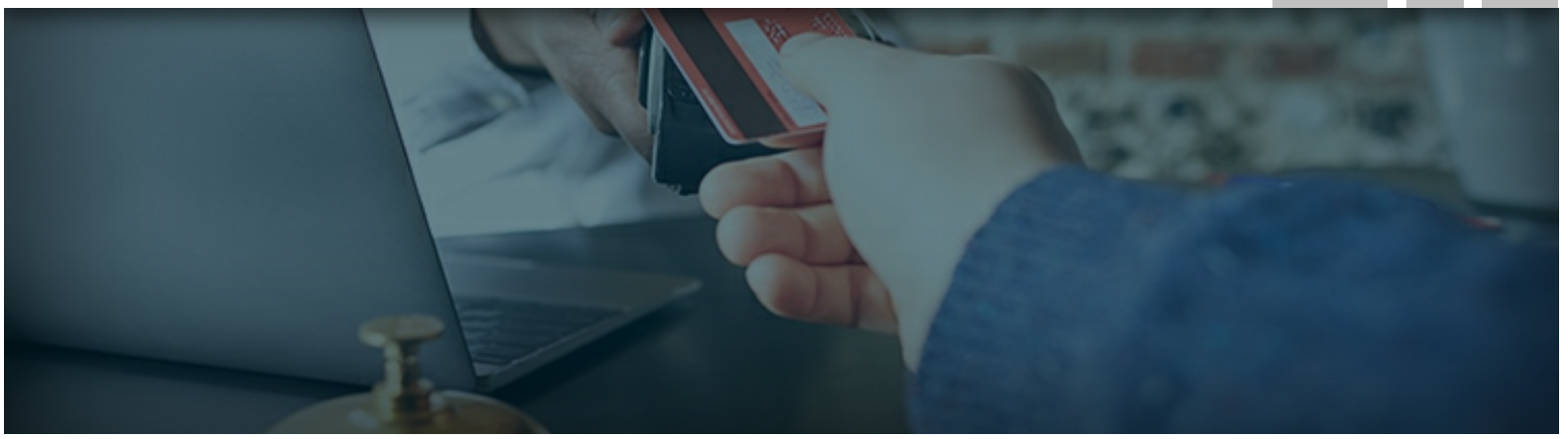

May 22, 2017

Third-party hacks expose businesses of all sizes to prospect of cyber attack

Sabre breach rattles wide web of interconnected networks, puts fresh focus on risk management

FEATURED STORY BY RODIKA TOLLEFSON, THIRDCERTAINTY

The breach of Sabre Corp.'s hospitality unit —which could impact tens of thousands of hospitality businesses—is the latest example of the potential ripple effects from a third-party breach.

But the breach, which Sabre disclosed to the U.S. Securities and Exchange Commission on May 2, is not just a reminder about the pervasiveness of this kind of risk.

Much of the focus in the discussion of third-party risk focuses on potential data theft. Less scrutinized is the risk stemming from the interconnectivity of the

networks, says Brad Keller, senior director of third-party strategy at Prevalent, which provides third-party-risk management.

Related article: *Why third-party risks need full attention*

Sabre reported "unauthorized access to payment information contained in a subset of hotel reservations" processed through its hospitality system. The reservation system is used by more than 32,000 properties, from small hotels to major chains. It also interconnects with more than 100 applications for property, revenue, content or customer relationship management.

Keller calls this the spider web effect—where one system services many clients, and the separate systems talk to one another. One breach can give hackers access to multiple companies.

Brad Keller, Prevalent senior director of third-party strategy

"It's not just a question of the data on an individual system—it's, 'where else can I go into this spider web network once I get into one spot,' " he says.

In its quarterly Securities and Exchange Commission filing that disclosed the breach, Sabre said it couldn't reasonably estimate at this time whether it will incur any liabilities due to the incident. But one has to look only as far as Target to see the magnitude of the damage that could arise from a third-party breach.

Outsourcing opens door to hackers

The risk is becoming more pervasive because of the growing trend in outsourcing, Keller says. As in any line of business, cyber criminals are looking to maximize their return on investment, which makes vendors an attractive target. In the case of someone like Sabre, it isn't about the company size but about the access it could provide.

"They (cyber criminals) look for vendors that service a lot of companies but may not be that large and may not have the kinds of resources necessary to keep everything in check," Keller says.

The spider web effect also compounds the problem because of the many layers of vendors in the supply chain, or what some in the industry refer to as Nth party because it's unknown how many layers deep the outsourcing is.

"When you start trying to count the layers in the spider web, you don't know how far it goes, and the further it goes, the knowledge drops for the (original) company," Keller says.

Risk not on radar enough

A survey of risk in the third-party ecosystem by the Ponemon Institute found that most companies don't have an inventory of all their third parties. At the same time, respondents believed that more than a third of their providers shared their sensitive information with Nth-party vendors. Only 20 percent knew how their data was being accessed and used by those vendors they didn't have direct relationships with.

Despite the growing awareness about third-party risk, it's still not on the radar of many businesses. Deloitte's 2016 survey on global outsourcing found that cyber risks affected outsourcing decisions only for 23 percent of respondents. In a perhaps more encouraging sign, half said they were modifying their outsourcing processes to focus on security risks and protocols.

Keller is seeing a shift in how larger companies are addressing this risk. Not only do they have security assessments for their own vendors, they also are requiring these vendors, in turn, to have robust risk-management programs for their providers.

"Not only do (vendors) need to have good programs in place and respond to assessments, but they need to have their own program so they're managing, effectively, the risk of any work that they're outsourcing—and can demonstrate that to their client," he says.

Regulators, too, are paying more attention. In health care, HIPAA was extended to business associates and the Department of Health and Human Services began putting more emphasis on business associate agreements. In banking, the state of New York turned the heat up a notch with its new cybersecurity rules, requiring written due diligence and warranties related to third-party providers.

Letting insurance cover risk

With the growing trend of cybersecurity insurance, more organizations will be looking at shifting some of their third-party risk. Sabre is a good example. In its SEC filing, the company stated that it has insurance that covers "certain

aspects" of the risk, and it was working with its insurance carriers on this matter.

But Keller, who was once an insurance defense lawyer, is skeptical that insurance is the answer. He says the vendor business partnerships are about revenue preservation—ensuring the business is not losing a revenue stream because of a breach. And, he adds, there's one other type of unrecoverable loss.

"Target was a good example," he says. "You can recover a lot of costs, but how do you recover the damage to your reputation?"

More stories related to third-party risk:

SMBs need to bulk up security to protect against third-party risk
Despite record breaches, secure third-party access still not an IT priority
Third-party vendors are the weak links in cybersecurity

Posted in *Cyber insurance* , *Data breaches* , *Featured Story*