



Hacking the Call Center

PCI, breach fears shine light on dark corners of call center insecurity

JUNE 26, 2008 | 4:10 PM

By **Kelly Jackson Higgins**
Senior Editor, *Dark Reading*

Hold the phone: Your call center handles sensitive data, too.

The contact center mostly has been forgotten as a potential point of breach -- even though customer service representatives take credit card numbers and outsourced help desk workers have access to your databases.

That all soon could change. The Payment Card Initiative (PCI), for instance, also applies to call centers that handle credit card data, so PCI is driving a new generation of security tools that encrypt voice call recordings of phone transactions. RSA's encryption technology, for instance, is now used to encrypt audio recordings handled by call center software vendor Verint Witness Actionable Solutions's call recording applications.

Even so, not all call centers are tuned into PCI, especially the smaller organizations. "We still find a real lack of awareness in the contact center community about PCI," says Kristyn Emenecker, director of solutions marketing for Verint, who says it's mostly the company's largest call center customers that have been asking about PCI so far.

Verint's software records calls in the centers. "Because that data is in an unstructured format -- a Wave file, for example -- companies are just starting to realize that it becomes an area of potential liability for them," Emenecker says.

Other products are emerging that come with a "blackout button" feature that prevents the credit-card number from being recorded on the call and thus not stored at the call center, for example.

But credit card information isn't the only exposure risk at these sites. Outsourcing-based call centers for IT and help desk support pose even more security problems. "This is a bigger and often more overlooked area, where PCI is not an issue. Credit card numbers aren't involved, but a major issue is they have access to or a copy of your customer database," says John Pescatore, vice president and research fellow at Gartner. "And many call centers that are outsourced use shared services. The same IT infrastructure that supports you is supporting" other organizations.

"External call center [employees] are not your employees. How do you know they're not going to go surfing through your data?"

Pescatore says there indeed are insider risks, but even more likely is human error causing a breach. "Someone looks up company A's customer, but mistakenly finds [a similar name] in Company B's database," he says.

That's a scenario where security tools like database monitoring, for example, would come into play. Database monitoring also would catch foul play by a call center worker. "A customer service representative typically has access to only one customer at a time... So if you see him retrieving 1 million customer records at once, that's not a CSR behavior pattern and the database activity monitor would detect that deviation," Pescatore says.

And just because you have an in-house call center doesn't mean you're more secure. The Yankee Group says in the next five years, over 50 percent of contact center agents in North America will be working

from remote locations -- like home -- at least two days a week, as companies move to less expensive, virtual call center models. How those workers handle sensitive data from their home offices, often attached to home computers, will become a big issue, according to Ken Landoline, program manager for The Yankee Group.

Landoline says some call centers already "black out" sensitive account information from the agent's view -- allowing a customer to punch in his passcode, for instance, that the agent can't see. That's another way to secure sensitive data: "Keep the agent removed from the secure interaction with the customer," he says.

Meanwhile, some third-party outsourcing call center firms overseas use older technology, which also leaves you exposed. "We've even seen some that use Telnet," says Cheryl Traverse, president and CEO of Xceedium, which sells a product that secures the channel between the call center and the caller.

Traverse says organizations should take care to secure their outsourced IT or help desk call center operations. "It's very important to put in best practices security in the call center not just for PCI, but also in general because these people [in IT support call centers] are often remotely located and not trusted personnel that do have the ability to compromise your critical infrastructure through the use of their [technical] skills," Traverse says. "You should also compartmentalize the support people only to areas they should be working with... They should not have visibility into the rest of the infrastructure."

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

- [RSA Security Inc.](#) (Nasdaq: EMC)
- [Gartner Inc.](#)

Copyright © 2008 United Business Media Limited - All rights reserved.