PHYS.ORG

Rise of outsourcing poses new cybersecurity problems

November 10 2011, By Steve Alexander

Big banks, hospitals and insurance companies worry about computer security because they handle so much personal information.

Now, in the age of outsourcing, they also have to worry about whether their partner firms are secure. And that's created a new kind of business consultant: The information security auditor who determines how much security is enough.

Some of these auditors work for big companies. When Evan Francen did security audits for Wells Fargo bank, he asked the outsourcing companies to complete a 1,500-question security checklist. (Wells Fargo officials declined to comment.)

Now Francen has his own security firm, FRSecure of Chaska, Minn., that helps outsourcing firms meet the demands of security auditors like him. And some of them really need the help.

"We audited a small bank that was compliant with computer security regulations, but we could have put them out of business in five minutes because of the physical risk," Francen said. "Their computer server room had no camera surveillance, no records of who came or went, no locked doors, nobody there at night, and it was in a separate building."

Such insecurity represents a business opportunity for the likes of FRSecure.

"We're in the Wild West period of security compliance," said Kevin Orth, FRSecure's vice president of operations. "There are no security standards that are widely accepted."

The opportunities in security auditing also have drawn the consulting arms of big accounting firms such as the accounting firm Deloitte.

"Every time there's another computer security breach, these security audit programs get ramped up quite a bit," said Matt Marsh, a partner in enterprise risk services at the Minneapolis office of Deloitte. "Because if there's a breach there can be costs, loss of reputation and loss of business."

Driving the latest corporate fear about computer security is a confluence of events. Computer security breaches, such as the massive e-mail leak this year at corporate outsourcer Epsilon, have become common. Cloud computing, which saves companies money by letting them use remote data centers when needed, poses new security risks about which little is known. And big companies are under more regulatory and legal scrutiny.

"All of those factors are converging, and are putting a lot more pressure on banks and other big companies," said Avivah Litan, an analyst for Connecticut research firm Gartner Inc. "Security audits have definitely taken a big upward tick."

For IT consultants, this is a boon. "Performing security audits is now a specialty within information technology consulting," said Isaac Cheifetz, an IT recruiter with Open Technologies Consulting Co. in Minneapolis. Security "is no longer simply about making sure the network firewall is up."

Added Marsh, "That whole space of security and privacy is a growth area for us."

That can drive consulting prices upward.

"We see many IT consultants trying to dabble in information security, and they set their prices at what their clients are used to paying," Orth said. "We make more, but we're specialists. So there's no such thing as standard pricing."

These days, consultants are called in when outsourcers find it difficult to meet confusing and sometimes excessive security demands of big companies for which they handle data.

"A lot of these security rules were written by non-IT people, and they aren't specific enough to give IT professionals a clear idea of how to set up security - and there are a lot of different ways to do it," said Aric Bandy, CEO of Agosto Inc., a Minneapolis IT outsourcing company that does work for Goodwill Industries, the Minnesota Wild professional hockey team and Dunn Bros. Coffee.

"One client wanted us to ensure we had control of who was physically able to access a computer server in our data center," Bandy said. "We already had card access to the data center, personal identification numbers for data access and a guard. But that wasn't enough: They wanted a camera focused on that server, and we had to do that."

Some outsourcers try to spare themselves that kind of anguish by launching a pre-emptive strike: They hire a company such as FRSecure to do a security assessment and develop a security plan that may help ward off some of the more unnecessary security demands of big clients.

"We'll do a security assessment so the vendor can push back on the security demands of the big company," Orth said. For example, if data encryption is too expensive, an outsourcer should develop a less-expensive alternative, such as surveillance cameras or documented procedures to destroy old disk drives, he said.

That strategy worked for FRSecure customer Action Inc., a Plymouth, Minn., direct-mail company that works with banks, health care institutions, insurance companies and schools.

"The first time you get audited for security, it can be a bit onerous," said Tony Zirnhelt, Action president. "But now we've taken a proactive approach to data security, such as employee training, cameras, data access control, even hiring someone to try to break in through our computer security. We now use our data security in our pitch to prospective clients."

That may be the most practical solution at a time when data security is so ill defined, said consultant Marsh.

"You could encrypt and secure everything to the nth degree, but that would cost a lot of money," Marsh said. "So there's a balance, and each institution has to figure out what that balance is."

Citation: Rise of outsourcing poses new cybersecurity problems (2011, November 10) retrieved 10 April 2024 from
https://phys.org/news/2011-11-outsourcing-poses-cybersecurity-problems.html