

Clarke Warns of Corporate Risk in Identity Theft

July 14, 2005
By Dan Briody



Richard Clarke can't avoid being controversial. After he released his scathing critique of the Bush administration's anti-terrorism policy, "Against All Enemies" (Free Press, 2004) early last year, a media firestorm engulfed him.

Yet, throughout it all the former Special Advisor to the President on Cyber Security has remained steadfast in his opinions. "This administration is still in the 20th century," he says.

Today, as chairman of his own cyber-security firm, Good Harbor Consulting LLC, in Arlington, Va., Clarke is more concerned with identity theft than with Al Qaeda. But he still can't pass up an opportunity to needle his old boss.

CIO Insight: Why aren't businesses that use private customer data held financially responsible if that data is stolen?

Clarke: Well, it depends on the company. When a bank or credit card company loses information and the account is debited as a result, the banks will make good on that debit. But if it's a data mining company, then they don't make good on it. In some cases people have grounds for a tort, but most average people don't do that.

What needs to change?

I think the Congress this year will pass a notification law like California's [which requires companies to notify customers in a timely fashion when their data has been compromised]. So there will be a federal law.

But there needs to be a good definition for the threshold of what exactly constitutes a breach. And we need a better definition of "timely." Neither are in the California law.

Does simple notification go far enough?

The California law is good. If it weren't for that we wouldn't know half of what's going on out there. But Congress should consider the new Japanese law, which says that if you have privacy data on more than 5,000 people, including employees and customers, then you have to adhere to a higher level of IT security.

Of course, the issue arises as to how anyone would know if a company was complying. The answer would be one of two things: a self-certification that a company would file with the Securities and Exchange Commission, or the SEC could check for compliance as part of an annual SOX audit.

What else?

I think we need to go a step further than the Japanese law. We need to ban private companies from using Social Security numbers as identifiers. And in Hong Kong they now require that all online consumer financial transactions require two-factor authentication (something in addition to a password).

A lot of identity theft is the result of spyware and phishing—basically stealing passwords. If you require just one more authenticator, it reduces the theft rate dramatically.

What kind of a job is the current administration doing in cyber-security?

The government doesn't have any serious efforts to implement a national strategy on cyber-security. There is a lack of federal funding for cyber-security R&D.

They have never understood this issue. They are so worried about body bags, and they don't understand that one thing leads to the other.