eWEEK
THE ENTERPRISE NEWSWEEKLY
August 30, 2006

IT Pros Say They Can't Stop Data Breaches

Updated: **Nearly two-thirds of respondents in a new study say they're ineffective in preventing data breaches.**

By Deborah Rothberg

In the wake of widely publicized security compromises at AOL and AT&T, a study released Aug. 28 by the Elk Rapids, Mich.-based privacy management research company Ponemon Institute finds that only 37 percent of IT professionals believe their company is effective at detecting data breaches.

Citing a lack of resources and high product costs as barriers to preventing data leakage, respondents were uncertain about their company's ability to discover breaches of confidential information. Only 43 percent believed that their company would detect a large breach (involving more than 10,000 customer records) more than 80 percent of the time. 17 percent of respondents felt their company would correctly detect a small data breach (involving less than 100 customer records) more than 80 percent of the time.

"We've gotten pretty good at protecting from spam and viruses. But, when you rob a bank, you go for the money, and that's the data. Companies are beginning to shift their priorities away from the perimeter and onto the information content," said Gordon Rapkin, president and CEO of Protegrity, a Stamford, Conn.-based provider of enterprise security management solutions.

Respondents viewed the loss or theft of customer or consumer data as the second most detrimental data breach, even if privacy laws required notification, diminishing brand, reputation and customer confidence, and making the incident a public event. The loss or theft of intellectual property came in first in terms of risk, reputations and cost to the organization.

Rapkin attributes many of the recent data breaches to what he calls our "Culture of Security."

"People just don't get it. If you think about our IT culture, you wouldn't think of putting together a PC today without anti-virus software or a network without a firewall, but we still think we can create a database and not protect it. This is where the culture hasn't matured; we're protecting everything but the data, and we need a cultural shift."

Though 66 percent of respondents reported the use of technologies to help their organizations manage the leakage of sensitive or confidential information, cost was the primary reason cited why organizations would not use these technologies. Thirty-five percent felt that they were too expensive, 16 percent felt manual procedures were adequate, 16 percent felt that their organizations were not vulnerable to breaches and 12 percent criticized existing technology-based data for having too high of a false positive rate.

"It's interesting that they claim cost as a reason they're not taking greater precautions. An earlier Poneman study found that the average data breach cost $13 million, and I estimate that this AT&T one will cost way more. Companies are still thinking 'it's not going to happen to me,' worrying about protection and not prevention," said Rapkin.

Many respondents believed that their organizations did not have the right leadership structure or enough resources to properly enforce compliance. Forty-one percent believed that their organization was not effective at enforcing compliance with their organization's data protection policies and procedures.