e-retailers' blasé on fraud prevention

Despite online fraud costing North American companies $US3.5b per year, 40 percent of online retailers have no fraud prevention in place and a significant percentage expend minimal energy trying to stay ahead of cyber criminals.

These worrying statistics come from a study of 200 business managers and IT executives in the USA in retail and financial services organisations conducted for ThreatMatrix, a provider of cybercrime prevention technologies, by Info-Tech Research Group. Somewhat paradoxically the survey found that 85 percent of online retailers considered fraud prevention to be a high priority.

The good news, it seems, is that most organisations are moving swiftly to implement systems designed to detect and prevent online fraud. The study found that half of the organisations that had no online fraud prevention processes and systems intended to implement these in the next twelve months.

"In the next year, only nine percent of companies surveyed will have no online fraud prevention processes and systems in place," it concluded.

"Most organisations had baseline IT security tools in place, including internal firewalls, endpoint and gateway anti-virus or malware protection," the report said. "Far fewer organisations had highly specialised IT security tools such as fraud prevention for online transactions, security management systems, content filtering, data leakage protection, and application control."

Info-Tech reported, "When it came to specifically preventing online fraud, respondents most often used network or application firewalls, network user monitoring, authentication and identity management systems. The online fraud prevention tools that received the highest performance ratings were internal firewalls, gateway firewalls, endpoint, and gateway anti-virus or malware protection."

The survey also revealed a disconnect between companies' approach to online fraud prevention and IT security in general. A relatively high 69 percent of respondents indicated that online fraud prevention at their companies was becoming more integrated with their IT security policies, processes and systems. However, companies still view online fraud prevention and IT security as distinct entities. Only 43 percent of respondents agreed that the distinction between online fraud prevention and IT security was blurring at their organisation; and 59 percent believed that IT security was more of a priority than online fraud prevention at their company.

According to ThreatMatrix, to provide the safest transactions for consumers, retailers need to screen transactions using previous transaction data to make better decisions about account takeover attacks; track transactions that are originating from a different country or IP address than where the account was created, and screen for customer identification verification at both account login and prior to transaction completion.

However with any implementation of security technology, a balance has to be struck between the assessed risk and the cost of prevention and protection. According to Visa subsidiary CyberSource's 2013 Online Fraud Report "Online Payment Fraud Trends, Merchant Practices, and Benchmarks," the companies surveyed reported an average annual loss through fraud of 0.9 percent of online revenue, leading CyberSource to estimate the loss across the US and Canada at $US3.5b.

The report said that by far the biggest cost in online fraud prevention was manual review of orders. Typically one in four orders are manually reviewed, and the staff resources to do this

To find out more about mobile sales force management visit: salesatwork.com

From: Trade Promotion Management News

Contacts

Paul Hosking
5426 4786
mailto: paulhosking@mailcaster.com.au