Half of financial institutions tolerate losses caused by cybercrime

According to a survey conducted by Kaspersky Lab together with B2B International in 2014, 52% of financial companies reimburse customer losses caused by internet fraud without actually investigating the circumstances. Almost a third of companies believe the costs incurred by cyber threats are less than the cost of protection. As cybercriminals increasingly target e-payments, this approach could translate into considerable expenses for the company.

Image: www.freedigitalphotos.net

Many organisations that work with online payments are prepared to accept the additional costs that arise from cyber-attacks. 28% of the representatives from financial companies and 32% of the online store employees polled are sure that the total losses from online crime, including reimbursement of stolen money, do not exceed the costs of deploying security solutions. Only 19% of financial companies and 7% of online marketplaces cite the cost of compensating customer losses in the top three most serious consequences of cyber fraud.

At the same time, according to Kaspersky Security Network, nearly 4 million users of Kaspersky Lab products encountered financial malware that attempted to steal their money in 2013 (a rise of 18.6% compared to the figure for 2012). In December 2013, a number of North American banks suffered losses of more than $200 million as a result of customers' bank card details and personal data being leaked - and the final sum of the damage is likely to be much higher. Obviously, the continued growth in cybercrime will lead to a situation where the compensation paid out by companies will exceed both the cost of protecting financial transactions and their compensation budgets.

"Besides the need for financial companies to set aside funds in their budgets to reimburse money stolen from customers, they also have to cover the costs of dealing with customer complaints. But most importantly, even if the victims are reimbursed quickly, they are likely to think twice about using the services of a bank that can't ensure their online accounts are secure. It is better to prevent the loss rather than compensate it," commented Ross Hogan, Global Head of Fraud Prevention Division, Kaspersky Lab.

"Customised solutions designed to protect online transactions such as the Kaspersky Fraud Prevention platform can reduce

the risk of online fraud to a minimum, meaning funds set aside for compensation can be freed up and used for developing the business."

Made up of several components, the Kaspersky Fraud Prevention platform provides multi-layered protection against today's financial cyber threats. Kaspersky Fraud Prevention for Endpoints provides protection for client devices running Microsoft Windows, Mac OS X, Android or iOS. Kaspersky Fraud Prevention SDK tools help financial institutions develop their own mobile apps that are protected by Kaspersky Lab's advanced technologies. The server part of the platform, Kaspersky Clientless Engine, helps prevent illegal transactions by analysing payment data and identifying attempted cyber-attacks, even if there is no security solution on the client device. Kaspersky Fraud Prevention includes additional services to keep companies informed about financial cyber threats and the measures that can be used to combat them, as well as providing assistance when investigating financial incidents.

Yet another compelling argument in favour of using specialised security solutions is customer negligence. According to another Kaspersky Lab survey, 57% of users pay little or no attention to the security of their online payments because they believe all the necessary measures are taken by their bank. This merely increases their chances of falling victim to cybercriminals.