

Insider risk problem revealed

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

Security experts have turned the notion that so called "malicious insiders" are the biggest cyber security threat for companies on its head.

The security vendor RSA revealed that the majority of breaches are actually caused unintentionally by employees.

Its survey showed that firms believed 52% of incidents were accidental and 19% were deliberate.

"Unintentional risk gets overlooked, yet it's the most serious threat to business," said the RSA's Chris Young.

"The sexy incident where someone gets arrested for stealing records and selling them to a third party for a lot of money is the stuff that catches the attention of the media, the regulators, executives and Congress people.

"But this is not necessarily where organisations have 100% of the risk," said Mr Young, the RSA's senior vice president of products.

The study conducted by the RSA and IT analysts IDC looked at 11 different categories of risk ranging from malware and spyware to employees having excessive access to systems and from unintentional data loss to malicious acts for personal gain.

The report concluded that the difference between the most frequent type of cyber breach - unintentional data loss, at 14.4% per year, and the bottom of the list - internal fraud, at 10.6% - is a clear sign that no single solution can address all potential internal security risks.

It covered over 400 firms from the US, UK, France and Germany across a variety of sectors including the financial industry, healthcare, telecommunications and technology.

'Weakest link'

The report noted that whether the threats are accidental or deliberate, the cost to a company of a cyber breach is still the same.

The RSA and IDC said disclosure of sensitive information results in regulatory actions, failed audits, litigation, public ridicule and competitive fallout.

"The figures are hard to quantify, but the average annual financial loss to insider risk adds up to \$800,000 (£480,000) overall per organisation in the US and between \$300,000-\$550,000 (£180,000-£330,000) in the UK, France and Germany.

"And that ties into the billions of dollars range when you think of the thousands of companies that comprise the IT industry," said Mr Young.

A recent report by the Ponemon Institute found that the average cost of a data breach in 2008 was \$202 (£122) per customer record.

The information security firm also determined that the expense continued to rise by 38% between 2004 and 2008.

The RSA and IDC discovered that the weakest link in any company is the temporary employee or contractor.

"They represent the greatest internal risk," Mr Young told BBC News.

"Most organisations start with a principle of trust and you trust your employees to be able to do their job

well and protect the interests of the company. There are always levels of trust which is greater or lesser depending on how closely tied an individual actor is to an individual organisation.

"It's likely contractors may be less well-trained in organisational policy and it's harder to maintain control over their access to systems because of the time they interact with an organisation. There is always a tension between letting an employee do his or her job versus security," said Mr Young.

The Better Business Bureau has drawn up a list of simple things companies should do to secure its data, often regarded as the crown jewels of any company.

It advises limiting systems access to a few trusted employees, using a password protection system for logging in, equipping computers with firewalls and virus protection and educating employees.

Story from BBC NEWS:

<http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/8215467.stm>

Published: 2009/08/25 13:20:06 GMT

© BBC MMIX