Exemple de document écrit en anglais

Upsurge in hacking makes customer data a corporate time bomb

By Peter Apps

(Reuters) - With hackers stealing tens of millions of customer details in recent months, firms across the globe are ratcheting up IT security and nervously wondering which of them is next.

The reality, cyber security experts say, is that however much they spend, even the largest companies are unlikely to be able to stop their systems being breached. The best defense may simply be either to reduce the data they hold or encrypt it so well that if stolen it will remain useless.

Only a few years ago, the primary IT security concern for many large corporations was stopping the loss or theft of physical disks or drives with customer information. Now, much harder to detect online thefts are rife.

Last week, Reuters revealed a host of big name U.S. Fortune 500 companies were on a hiring spree for board level cyber security experts often offering $500,000-700,000 a year, sometimes more.

Many have high-level backgrounds, at much lower pay, at signals intelligence agencies such as the U.S. National Security Agency or Britain's GCHQ - although security experts say European firms are reluctant to hire ex-NSA staff following revelations over the scale of U.S. cyber monitoring by whistleblower Edward Snowden.

"Information has become toxic for retailers because the more they have, the bigger a target they become," said Lamar Bailey, security researcher at IT security firm Tripwire. "The ongoing rash of attacks brings into question what information an organization should be keeping."

U.S. retailer Target ousted its CEO Gregg Steinhafel in May after the firm said foreign hackers had stolen up to 70 million items of customer data including some PIN numbers late last year.

Industry watchers said purchases on its website dropped noticeably in the run-up to Christmas with the breach also sparking lawsuits and official investigations.

A report from cyber security think tank the Ponemon Institute showed the average cost of a data breach in the last year grew by 15 percent to $3.5 million. The likelihood of a company having a data breach involving 10,000 or more confidential records over a two-year period was 22 percent, it said.

The corporate fallout from the largest recorded breach so far, the loss of password data on some 145 million customers from online retailer eBay, is not yet clear. A senior eBay executive told Reuters last week that "for a very long time" the firm had not realized customer data had been seriously compromised by the attack.

June 9, 2014