INSURANCE JOURNAL

Company Data Breach Now Costs $3.5M on Average: Ponemon Study

May 7, 2014

The average cost of a corporate data breach increased 15 percent in the last year to $3.5 million, according to a study.

The study by the Ponemon Institute out of Michigan also found that the cost incurred for each lost or stolen record containing sensitive and confidential information increased more than nine percent to a consolidated average of $145.

The study says that companies that said they have a strong security posture were able to reduce the cost by as much as $14 per record.

Consistent with Ponemon's previous studies, the most common cause of a data breach is a malicious insider or criminal attack. However the causes of data breaches vary by country and also include human error and system failures, according to the report.

The most costly data breaches were those caused by malicious and criminal attacks. Companies in the U.S. and Germany paid the most at $246 and $215 per compromised record, respectively.

The Ponemon Institute's ninth annual Cost of Data Breach Study: Global Analysis, tallied responses from 314 companies spanning 10 countries.

"The goal of this research is to not just help companies understand the types of data breaches that could impact their business, but also the potential costs and how best to allocate resources to the prevention, detection and resolution of such an incident," said Dr. Larry Ponemon, chairman and founder of Ponemon Institute.

This year's Cost of Data Breach Study also provides guidance on the likelihood an organization will have a data breach. The study is sponsored by IBM.

INSURANCE JOURNAL

Among the study's other key findings:

• The most costly breaches occurred in the U.S. and Germany at $201 and $195 per compromised record, respectively. The least expensive data breaches were in India and Brazil at $51 and $70, respectively.

• Root causes of data breaches differ among countries. Countries in the Arabian region and Germany had more data breaches caused by malicious or criminal attacks. India had the most data breaches caused by a system glitch or business process failure. Human error was most often the cause in the UK and Brazil.

• The appointment of a Chief Information Security Officer to lead the data breach incident response team reduced the cost of a breach by more than $6.

• The involvement of business continuity management reduced the cost of data breach by an average of almost $9 per record, the study found.

"Clearly, malicious insiders and criminal attacks are a growing concern for businesses, especially when we consider how persistent data has become in the age of cloud and mobility," said Kris Lovejoy, general manager, IBM Security Services Division. "A data breach can result in enormous damage to a business that goes way beyond the financials. At stake is customer loyalty and brand reputation."

Companies in the study said that the greatest threats are malicious code and sustained probes. Companies estimate that they will be dealing with an average of 17 malicious codes each month and 12 sustained probes each month.

Unauthorized access incidents have mainly stayed the same and companies estimate they will be dealing with an average of 10 such incidents each month.

Only 38 percent of companies have a security strategy to protect their IT infrastructure. A higher percentage (45 percent) has a strategy to protect their information assets.

Source: Ponemon Institute