HealthManagement
Promoting Management and Leadership

How to waste time and money - don't invest in cybersecurity

Data breaches impose higher financial burden on healthcare in comparison to other sectors, according to a new report, which underscores the need for organisations to invest in cybersecurity technologies to counter hacking threats.

According to Ponemon's "Cost of a Data Breach Report", a breach in financial services, the second most expensive sector, costs $206 per consumer. By contrast, hospitals end up spending about $408 per patient record as a result of attacks on their systems. That amount is higher than last year's $308 per patient record.

In the report, sponsored by IBM, Ponemon compared the cost of data breaches around the globe and across all sectors, and found data breaches cost organisations $3.86 million, up 6 percent from last year. Researchers spoke with more than 2,000 individuals and 477 organisations to calculate these costs.

Although the cost of data breaches fell year over year to $3.62 million, the report notes, those costs have once again increased – up from $141 per record across all sectors last year.

It’s also notable that data breaches are costlier in the U.S. than any other country, with an average of $7.91 million. For comparison, it cost Buffalo-based Erie County Medical Center nearly $10 million to rebuild its systems after falling victim to a ransomware attack in April 2017.

Healthcare organisations incur higher costs from data breaches mainly because of a loss of reputation, which leads to a lack of information, strained relationships with other businesses, education and a loss of customers. However, one of the biggest reasons is a loss of time, when employees are doing damage control after a breach, the report said.

In addition, the researchers found that incident response speed has a major impact on the overall cost of a breach. If a breach is contained within a month, organisations can save up to $1 million in comparison to those with slower response times, the researchers said.

And having an incident response team and plan, along with automated cybersecurity tools, also directly impacts the cost, according to the report.

"Organisations that had extensively deployed automated security technologies saved over $1.5 million on the total cost of a breach," the report found.

“There are many hidden expenses which must be taken into account,” explained Wendi Whitmore, global lead for IBM X-Force Incident Response and Intelligence Services. “Knowing where the costs lie, and how to reduce them, can help companies invest their resources more strategically and lower the huge financial risks at stake."

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 17 Jul 2018