Firms with significant cyber events see longer-term impact on stock value

By Erin Ayers, Front Page News

Cyberattacks can have “significant and sustained” impact on shareholder price, with firms that report significant cyber incidents underperforming the broader market by about 5% on average, according to a new study from ISS STOXX and ISS-Corporate.

“It is well known that cybersecurity incidents can have an immediate and meaningful impact on the share values of publicly traded companies,” said the authors of the report, titled *The Sustained Negative Impacts of Cyber Incidents on Shareholder Value*. “What’s less understood is the depth and duration of that damage and what kind of companies suffer the most.”

The researchers used the U.S. Russell 3,000 index, tracking companies over a three-year period between 2022 and 2024. A significant cyber event was defined as any event having impacted 10,000 or more individuals. They found that for a full year after an event, the share price underperformance persists for one full year after incidents are first reported with a peak gap of 4.9% after 250 trading days.

ISS researchers also found that a few industries experience greater negative impacts, including finance and banking and healthcare. The two sectors saw negative average impacts of 8.5% and 8.3%, respectively.

ISS noted that the prolonged stock impact highlights the importance of building resilience to cyber events.

“Cyber incidents are not just momentary annoyances or quickly forgotten news items,” said ISS. “Firms that report significant cyber incidents suffer material and sustained impacts to share price performance relative to sector and broader market peers.”