Target Breach Costs Could Reach $1Bn

February 28, 2015 Tara Seals US/North America News Reporter, Infosecurity Magazine

http://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn?utm_source=twitterfeed&utm_medium=twitter

The data breach at Target that affected 70 million US consumers has cost the retail giant $162 million in 2013 and 2014, and could end up totaling $1 billion or more in damages before all is said and done.

During its fourth-quarter earnings call, the big-box behemoth said that it booked $4 million related to the breach in Q4, and $191 million in gross expenses for 2014. It also spent $61 million gross for 2013.

While the gross expenses were in part offset by insurance receivables ($46 million for 2014 and $44 million for 2013), the losses look to only mount, as lawsuits begin to be filed. Plaintiffs were given the go-ahead for class-action litigation by a judge in January.

“The major breaches such as Target, Sony and Anthem damage brand reputation and consumer trust, but they also have a real impact on the bottom line,” said Eric Chiu, president and co-founder of HyTrust, in an email. “The $162 million spent so far by Target is just a drop in the bucket given the class-action lawsuits by consumers as well as the recent court ruling that banks can go after Target to recoup their losses.”

The annual M-Trends report from FireEye noted that the huge number of targeted attacks last year were disproportionately aimed at US retailers. At 14%, retailers accounted for the second largest number of Mandiant engagements in 2014, after business and professional services (17%). This was a rise of 10% from the previous year.

Weak authentication when accessing virtualized application environments was found to be a major attack vector in the retail sector, allowing hackers to gain an initial foothold into systems from which they could “roam into other parts.” It’s an avoidable problem that Target famously has exemplified, leading to several resignations in its C-suite.

“Invest now or pay later—this is the message from one of the largest data beaches reported to date,” said Steve Hultquist, chief evangelist at RedSeal, the security analytics company. “Consider the ROI for even a very significant investment in proactive security analytics and process improvements that could have blocked the breach before it even started.”

As Hulquist nutshelled it, “The lesson for other organizations is clear: you are under attack. Making strategic investments now is a wise preventative measure to keep your organization and your customers safe.”