Data breaches: A new source of worry for CEOs

May 6 2014, by Bree Fowler

This undated file photo provided by Target Corp. shows the company's chairman, president and CEO Gregg Steinhafel. Steinhafel is the first boss of a major corporation to lose his job over a theft of customer data. His exit from the helm of the nation's second-largest retailer on Monday shows that -- in addition to guiding company strategy and keeping Wall Street happy with ever-growing profits -- today's chief executives are being held responsible for lapses in computer security. (AP Photo/Target Corp., Johansen Krause, File)

Add hackers to the long list of things that give chief executive officers insomnia. Target's chief executive, Gregg Steinhafel, is the first boss of a major corporation to lose his job over a theft of customer data. His exit from the helm of America's third-largest retailer on Monday shows that—in addition to guiding company strategy and keeping Wall Street happy with ever-growing profits— today's chief executives are being held responsible for lapses in computer security.

Daniel Ives, an analyst for FBR Capital Markets, believes many CEOs will be placing calls to their chief information officers today, just to make sure their operations are as fortified as possible.

"Ultimately, it's the CIO and the IT managers that are really more in the weeds," Ives says. "But just like the head coach of a football or basketball team that doesn't make the playoffs, the CEO is ultimately responsible."

Steinhafel was in charge when hackers stole millions of consumer data records, including credit card number, names and addresses, from Target's computer system last holiday season.

To be sure, Target had been struggling with weak sales for several years and had run into problems with its Canadian expansion. But there's no denying the breach and its fallout were big factors in Steinhafel's departure, says Ronald Humphrey, a professor who studies leadership at Virginia Commonwealth University.

Humphrey believes that while a company's CEO is responsible for data security, the issue—much like worker security or environmental contamination—can sometimes get put on the backburner, because it isn't always recognized as a core part of operations.

"This is a wakeup call to CEOs that data security is something that

affects their customers," Humphrey says. "If you've had your identity stolen you know it's a huge headache. I think they have to take this very seriously."

And if a breach does occur, a CEO needs to be able to show his board of directors that it didn't result from a lack of resources devoted to data security, he says.

Minneapolis-based Target Corp.'s computer systems were infiltrated by hackers who took 40 million debit and credit card numbers, along with the personal information of as many as 70 million people.

Target revealed in its fourth-quarter earnings release in February that it incurred $61 million in breach-related expenses. After the company received insurance payments, its net expenses for the hacking incident were $17 million. The company is expected to report additional charges when it releases its first-quarter results later this month.

Meanwhile, total costs related to the company, banks, consumers and others are expected to reach into the billions.

Investigations by both Target and the Secret Service are ongoing. Neither has released details about their probes and the Secret Service has said it could take years to bring the responsible parties to justice.

Target's revenue, earnings and stock price have all suffered since the breach's disclosure in December. Steinhafel's departure after a 35-year career with Target suggests the company is looking to make a fresh start in the aftermath of the breach. Chief Financial Officer John Mulligan will take over as interim president and CEO. Roxanne Austin, a member of Target's board, will be interim nonexecutive chair of the board. Both will serve in those roles until the company finds permanent replacements.

Data security is becoming a top priority for the savviest of company leaders, especially those in data-driven industries like finance and retail, because it can do so much damage. Analysts expect businesses around the world to spend a combined $30 billion this year on cybersecurity.

Robert Hurley, a professor of management at Fordham University, says recent weak store traffic and the company's problems in Canada were probably equally big factors in the Target board's weighing of Steinhafel's fate. He says he doubts the board would have pushed for a change if the breach was the only problem involved.

But Hurley adds that the breach was a major event that damaged Target's reputation and credibility with customers. That damage likely prompted the board to act. Hurley credits the board with taking its time and not making a knee-jerk decision.

"It's a good example of board governance," Hurley says. "I think they realized that there are too many strategic barriers and that a new CEO would help solve their problems."