

INSIGHT ON BUSINESS

HACKERS INFILTRATE TARGET



In today's marketing and advertising landscape, companies spend billions building goodwill with their customers and improving perceptions of their brand. When data breaches occur, the short-term monetary losses can sometimes pale in comparison to the damage to their reputations and to the brands that they work so tirelessly to build. In 2014, retailing giant Target learned this firsthand when the company experienced a data breach rivaling some of the biggest on record. Renowned for its positive reputation among customers, Target is still suffering the financial and reputational consequences for the breach. The company has been heavily criticized for its response to the breach while it was still in progress, and to a lesser extent for its handling of the breach in its aftermath.

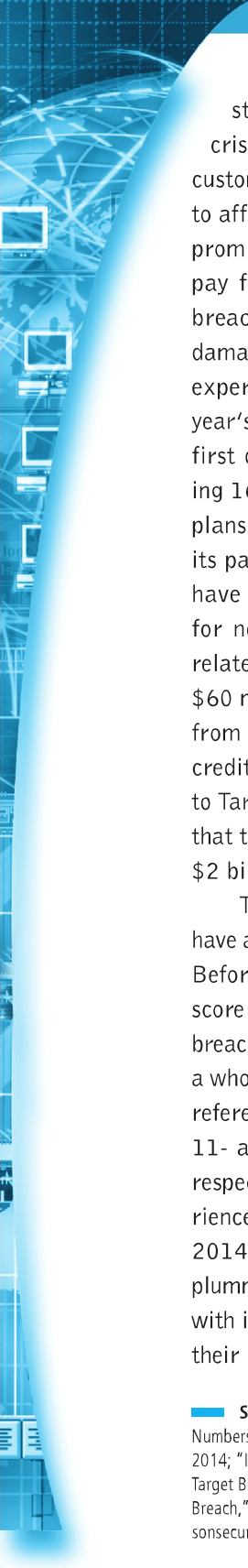
In late 2013, in response to speculation from industry experts and security professionals, Target confirmed that it had been the victim of a data breach that had compromised approximately 40 million consumer credit and debit cards. Target later admitted that other personal information such as mailing addresses, phone numbers, and e-mail addresses had been stolen for an additional 70 million people, bringing the total of affected customers to 110 million. Hackers had reportedly gained access to the full set of information corresponding to each stolen credit card, including names, card numbers, expiration dates, and CVV codes, as well as the PIN data for debit cards. Although Target claimed that these PIN numbers were encrypted and were still secure, the company advised customers who had shopped at Target during the time frame of the attack to monitor their credit and debit cards for suspicious activity. In the immediate wake of the breach, customers

quickly reported fraudulent charges from Russia and other countries across the world.

The attack took place over the course of several weeks during November and December of 2013, after hackers used network credentials stolen from a heating and air conditioning company that was a Target subcontractor, and installed malware within Target's security and payments system. The malware was a simplistic program that was created to steal card information and to reroute it to external servers. Anytime a customer swiped their card, the malware would grab the card's identifying information and store it on an internal Target server controlled by hackers.

This type of attack should not have taken Target by surprise. The company had just contracted with computer security firm FireEye to install a system intended to detect these types of malware attacks. On one of the first days of the attack, FireEye spotted suspicious activity and notified Target. Amazingly, Target's security team did nothing in response to the alert, preferring instead to just monitor the situation. Had they responded in a timely manner, they could have neutralized the threat well before any customer data left Target's network. In fact, a FireEye security feature would even have neutralized the malware automatically, but Target had opted to turn that feature off.

When Target finally acted to stop the breach in mid-December, the breach had grown to such size and scope that it was the second-largest retail cyberattack ever, rivaling past breaches of Heartland Payment Systems and TJX Companies. Security experts have expressed shock that Target could have allowed such a simplistic attack to do so much damage, characterizing both the attack and the attackers as amateurish at best.



Target initially gave customers a 10% storewide discount in the aftermath of the crisis to try and resurrect its reputation with its customers. It also offered free credit monitoring to affected customers, and CEO Gregg Steinhafel promised that no Target customer would have to pay fraudulent charges as a result of the data breach. Nevertheless, the data breach severely damaged Target's holiday sales, as the company experienced a drop of 46% from the previous year's figures, and that malaise continued into the first quarter of 2014, with sales figures declining 16% over the same period from 2013. Target plans to spend another \$100 million upgrading its payment terminals, and customers and banks have filed nearly 100 lawsuits against Target for negligence and compensation for damages related to identity theft. Combine that with over \$60 million and counting in costs to the company from promotions like the store discount and free credit monitoring, and the extent of the damage to Target becomes clearer. Some analysts estimate that the total damage to Target is between \$1 and \$2 billion dollars.

The data breach has also caused customers to have a crisis of confidence with respect to its brand. Before the day of the breach, Target's BrandIndex score was an excellent 25.8. In the week after the breach, its score was a negative 19.1, representing a whopping 44.8 drop in consumer perception. For reference, Citibank and Playstation suffered only 11- and 15-point drops in consumer perception, respectively, after the two companies each experienced a data breach in 2011. Midway through 2014, Target is still struggling to rebound from plummeting consumer sentiment towards its brand, with its scores measuring at approximately half of their levels prior to the breach.

Target has certainly been doing whatever it can to undo the damage. In March 2014, Target's CIO resigned, and the company announced an overhaul of its information security procedures. For many disgruntled customers and concerned analysts, this was an insufficient response, and more sweeping changes followed. In May 2014, CEO Steinhafel resigned as well, facing mounting pressure. Ironically, Target had already been bolstering its security, increasing the number of information security employees to 300 and opening a 24-hour operations center in charge of reviewing suspicious activity. Target selected Bob DeRodes, formerly a senior IT advisor for the Department of Homeland Security and CIO at Home Depot and Citibank NY Global Card Products Group, further indicating its commitment to information security. Ironically, just a few months later, Home Depot announced that it had also suffered a major data breach, extending from April to September 2014, the extent of which is not yet known, but perhaps may even surpass Target's.

Studies have shown that the average cost of a data breach has risen to \$3.5 million in 2014, and that number may continue to escalate unless companies improve their safeguards against these events. One issue for Target was that its manager of security operations had stepped down in the months preceding the attack and had not yet been replaced. If Target had had someone in that position, that person might have taken a more active role in neutralizing the breach. More than continuing to increase its level of investment in IT security, Target and other companies need to improve their internal processes so that when warnings and alarms are sounded, security teams take action, instead of sit idly by as Target did.

SOURCES: "After the Big Data Breach, Has Target Learned Its Lesson?" by Adam Levin, Abcnews.go.com, June 15, 2014; "The Target Breach, By the Numbers," by Brian Krebs, Krebsonsecurity.com, May 14, 2014; "Lessons from Target's Data Breach Fumble," by Jennifer Schlesinger, CNBC.com, May 11, 2014; "Introducing Target's New CIO Bob DeRodes," Abullseyeview.com, April 29, 2014; "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," by Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Bloomberg Businessweek*, March 13, 2014; "Target Missed Signs of a Data Breach," by Elizabeth A. Harris and Nicole Perloth, *New York Times*, March 13, 2014; "Target Hackers Broke in Via HVAC Company," by Brian Krebs, Krebsonsecurity.com, February 14, 2014; "Target Perception Falls After Data Breach," by Ted Marzilli, BrandIndex.com, December 23, 2013.