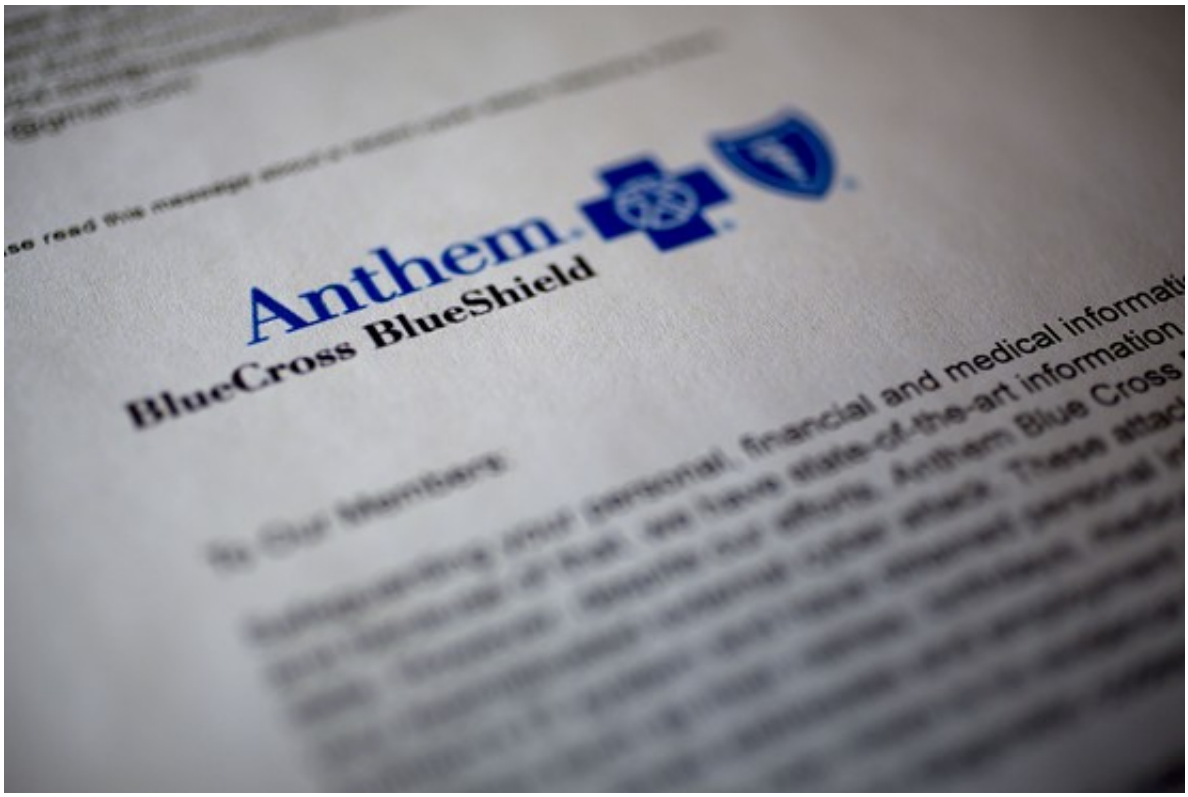
Risk & Compliance Journal.
THE WALL STREET JOURNAL

March 2, 2015, 4:22 PM ET

Crisis of the Week: Anthem's Breach Response Evaluated



Andrew Harrer/Bloomberg

A copy of an e-mail sent to Anthem Inc. plan members with notification of a cyberattack is arranged for a photograph.

It's been a few weeks since Anthem Inc. announced it had been breached, with nearly 80 million customers and employees potentially affected. The company is cooperating with investigators, and set up web pages to communicate with customers and employees. We asked crisis management experts to review the company's response to date, pointing out where it did well in communicating with its affected constituents and where it fell short.

Andrea Bonime-Blanc, CEO, GEC Risk Advisory: "Anthem's immediate corporate response to its cyberbreach crisis appears to be close to a textbook case of effective immediate crisis management and preparedness. First, Anthem actually discovered the breach themselves–they weren't extorted by the hackers or outed by the media or others. This is good reputation risk management.

"Second, Anthem immediately advised federal authorities of the breach and hired reputable cyber consultants to deal with immediate damage control. This, too, denotes the existence of internal preparedness. Third, although applicable regulations appear to allow for a 60-day reporting window, Anthem decided to publicly announce its crisis within days of its first discovery. While perhaps risky, such a move can provide Anthem with longer-term reputation enhancement with key stakeholders, restoring and building trust and customer loyalty over time.

"Fourth, the company provided clear and coherent messaging of what happened–down to the kind of information that might have been compromised–in easily available and clearly written materials, including special instructions and a website for the occasion. Fifth, the CEO letter is an effective letter, addressing the concerns of key stakeholders (employees, customers, regulators and investigators) and providing them with immediate resources. In the letter, the CEO also apologizes and brilliantly shows empathy with his customers and employees by referencing the fact that his personal data was stolen as well.

"The only downside that I can discern from what has been reported doesn't have to do with Anthem's crisis response but more with its risk preparedness regarding the apparent lack of encryption on the data that was stolen. However, this is more of a risk management issue that Anthem and its executives and board will now surely be focusing on as they begin build stronger cyber resilience."

Richard Levick, CEO, Levick: "Anthem was obviously aware of how critically important it is to publicly respond with maximum speed in the immediate aftermath of any privacy data loss crisis. Indeed, the company was praised by law enforcement for doing just that after its historic breach earlier this month. However, this need for speed can create communications that seem rushed, vague, or incomplete.

"On day one, it was apparent that the Anthem forensic teams had not been able to provide a more complete picture of the damage to include in the initial communication. In particular, the announcement only vaguely alluded to the size of the affected population as in the 'tens of millions' of customers. There was a further full-day delay before it was revealed that critical data was not encrypted.

"Most critically, Anthem neglected to separately contact stakeholder companies, prompting perhaps millions of people to flood their own human resources departments for information. This customer communications is key. One official at a client company told us he first learned of the breach by reading about it in The Wall Street Journal. While such important business relationships may not now be directly threatened, it is clear to us from a few confidential conversations that more was expected from one of the nation's largest insurers. For the industry as a whole, the imputed lapses create anxiety about how effectively other companies may handle

data crises in the future."

(Anthem sent Risk & Compliance Journal a response to Mr. Levick's claim the company failed to separately contact stakeholder companies. It said: "Our focus is to be transparent, accurate and timely in our communications with all of our constituents. … We issued an open letter to our members, both online at Anthemfacts.com, and directly via e-mails to various constituent groups, including our employer customers, timed in concert with the very first article that was published. … We immediately held multiple town hall meetings with thousands of employers and brokers, as well as individual meetings with regulators and large employers–sharing updated information and responding to questions. Finally, understanding the importance of our employer customers' needs to communicate, Anthem developed multiple toolkits that include FAQs and template memos that were used to distribute accurate information to our customers' employees.)

Daniel Diermeier, dean, Harris School of Public Policy, University of Chicago: "As in many major business crises, companies need to respond quickly and focus on reassuring customers and restoring trust. This requires an authentic response that is transparent, competent, committed and shows real concern for the fears and frustrations of customers, even if such fears may be overstated.

"Anthem's message from the CEO was appropriate and personal, but various questions–whether customers were notified sufficiently quickly, and some confusion on whether customers need to sign up for identity protection or if it is provided automatically–led to some doubts about the company's competent handling of the crisis.

"Customers will not be forgiving in cases of lapses or missteps. Such heated customer reactions in the context of hacking incidents may be puzzling, even upsetting to executives. After all, companies such as Anthem were the victims of sophisticated, organized criminals. Shouldn't the public have some sympathy for the company that has been victimized? In the case of Anthem's data breach that means that management will be solely evaluated on how well it takes care of customers whose data has been compromised, whether the company is ultimately responsible for the breach or not."

Write to Ben DiPietro at ben.dipietro@dowjones.com, and follow him on Twitter @BenDiPietro1.