MET HC 758 Assignment Three by Rachel Logan

Release Statement:

Anthem is the victim of the latest cyber-attack on health care. We believe names, birthdays, addresses, Social Security numbers, and employment data may have been stolen. Tens of millions of our customers could be affected. We are offering free credit card monitoring and identity theft to all our customers as we work with the FBI to understand this complex attack. We encourage all customers to visit our website AnthemFacts.com to find more information and to call our toll-free number with any questions or concerns: 877-263-7995. We apologize that this has happened; securing your information is our number one priority. We will be analyzing our security systems so we can improve our practices and earn back your trust.

Sincerely,

Joseph R. Swedish
President and CEO
Anthem, Inc.

5 Short Talking Points:

These talking points will be made by CEO and President Joseph Swedish. Because he has released the response statement, we want to make him the face of the company. We don't want to dilute the messaging by having too many different people delivering statements. By having Swedish release the response statement, give the five talking points, and post an extended letter on our AnthemFacts.com website, we believe this will create a strong, unified message.

1. What happened:

Anthem has been the latest victim on cyber-attack on health care. We believe that tens of millions of our customers could be affected. Attackers gained access to names, birthdays, Social Security numbers, and employment data. My own personal information was breached.

2. The Investigation:

Since the attack, we have been working closely with the FBI to close the breach and identify those who are responsible.

3. Helping the Affected:

In the meantime, we encourage all of our customers to visit our website Anthemfacts.com. There you will find more details and learn how to protect your information moving forward.

4. The Website:

We are offering free identify theft protection and credit card monitoring to our customers. Protecting your personal information is our number one priority at Anthem, and we want to give you peace of mind during this ongoing investigation. We ask our customers to remain vigilant of

piggy-back attackers. Anthem is not collecting any personal information at this time. Do not give your information to anyone who is presenting themselves as an Anthem employee.

5. Moving Forward:

We sincerely apologize to every one of our customers. Moving forward, we will be analyzing the systems we use to protect your information and improving our practices so you can confidently put your trust back in Anthems hands.

5 Challenging Questions:

1. How can we trust you that this attack won't happen again? Why should we trust you?
2. My information was stolen! What are you going to do fix this problem and protect my identity?
3. Why did this attack happen at Anthem? Were you cutting corners with security to save money?
4. Do you even care about your customers?
5. I read that you discovered this attack last week! Why did you wait so long to tell us? What else are you trying to hide?

Anthem Analysis

When Anthem's security was compromised in 2015, Anthem was in danger of losing all their customer's confidence and business. The carefully devised reaction and action carried out by Anthem's Public Information Officer (PIO) was crucial in restoring the public's opinion of Anthem and convincing customers to continue putting their trust in the company. By containing the story, creating the messaging, and cultivating the plan moving forward, Anthem did an excellent job of moving forward after this massive security breach.

Anthem was able to contain the story for several days before the news broke in the media, allowing the company time to devise a plan. The USA Today report stated that Anthem realized the breach in their security last week, but breach was not announced in the media until Wednesday night. During the time between the discovery of the breach and the email that went out to customers Thursday morning, Anthem's public relations team, PIO, and administration

were able to determine what would be the best path forward to not only announce cyber-attack, but to formulate a message that would resonate with stakeholders.

Anthem had time to create a messaging package that would speak directly to the customers who were affected and reassure the public that had heard about the breach. Anthem fist contacted its customers in an email that admitted to the attack and explained what data had been compromised. The email then directed customers to anthemfacts.com, a website created solely to address questions regarding the security breach. By preemptively creating a website, Anthem was able to gain control of the narrative it wanted to spin for its customers and curious public, instead of being put on the defensive.

The letter from CEO and President Joseph R. Swedish was cleverly written to speak directly to the key stakeholders of the breach: the customers and internal employees. Swedish describes the attack as "a very sophisticated external cyber attack." His choice of words paints the attack as seemingly un-preventable, as if it could have happened to any company, and it just happened to occur at Anthem. Swedish describes the swift action of the investigation and the company's partnership with the FBI. The involvement of the FBI immediately instills the idea that the best people are working on the problem; it also suggests that Anthem has nothing to hide if the company contacted the FBI to launch an investigation. Swedish writes that his own personal information stored at Anthem was compromised, placing himself down at equal level as his customers and employees; now there is a comradery in the midst of the unfortunate events. The letter ends with an apology and a phone number that allows those with questions to speak with someone directly.

The website centralizes information and provides a path forward after the attack. The website provides useful information in addition to the letter, including an extensive Frequently

Asked Questions area. The website also provides the next step for those affected: how to sign up for identity theft. A well-written letter by the President and CEO does not diminish the fact that sensitive information was stolen. The free identity-theft service offers customers a place to move forward.

Overall, Anthem did an excellent job of reacting to this massive security breach. When tens of millions of people are affected by a cyber-attack, there is no way to cover it up the problem. Anthem recognized this and acted accordingly by controlling the story, devising a message, and offering a path forward for customers in the wake the attack.