Discussion Questions: Anthem Case Study

1. Briefly explain what happened in the Anthem data breach
2. Compare the phishing schemes in the Anthem case and in the Target case, what are the things in common? And what are things different?
3. It's possible that attackers tried to compromise the Anthem network as early as April 2014, but were thwarted. However, they kept at it and eventually succeeded. How do you know if you really clean up the hacked network?
4. What are the common ways for backdoor attacks?
5. What is data dripping?
6. How does behavioral analysis help to discover the attack?
7. Can data encryption help to defeat the attack? Why or why not?
8. Is two factor authentication strong enough to defeat Anthem alike attacks?
9. Why hackers are targeting the medical sector?
10. What are the things Anthem did not do correctly? Please answer the questions from the security policy aspect.