**3. Analyzing the incentives of actors to take the countermeasure**

The incentives for the actors to employ the countermeasure highly depend on the distribution of costs and benefits among them. However, cost-savings that can derive as a result of the countermeasure can exceed the cost of implementation, something that also influences the decision of actors.

In the case of the problem owner, i.e. the security department of the organization, continuous vulnerability assessment and remediation is a time-consuming task to perform, however when implemented it can prevent disastrous incidents. On the one hand the organization has to think about the significant time, attention and resources that a continuous assessment requires (Sans, 2015). On the other hand it is known that firms which do not use this countermeasure have an increased likelihood of ending up with their systems compromised. Today this countermeasure can be implemented by frequently running automated scanning tools (Sans, 2015). Hence, the organization seems to have the incentive of “preventing the worse” to engage in this countermeasure.

As regards the developers, being continuously occupied with the vulnerability assessment sounds a daunting task since they have to pay extra attention and effort in order to code a safe application. Nevertheless, implementing this countermeasure can save considerable amount of time required for finding a solution to the security issue. Developers often have the appropriate knowledge in identifying vulnerability issues thus the continuous assessment can benefit them; since they are the ones to fix the plausible security “holes” in the applications, having monitored them from the beginning saves time to fix them. Especially for XSS and SQL injection attacks it was found that the average fixing time was 92 and 138 days respectively. Therefore, developers may have the incentive of long-term time-saving in order to take this countermeasure.