They talk about System Development Life Cycle and how to handle security during the process from requirements gathering up to the system testing. They haven’t included maintenance because this part is the repetition of all the processes.  
During requirements gathering, it is a must to adopt international standards that fit your organization, during system design, it is better to do an external review of all your design. For the implementation part, the coders must use a specific language that is more immune or less vulnerable to security issues, follow a security coding checklist, and develop a defensive application to manage different attacks. During the testing phase, it must have a security testing plan of your different components, testing of attacks that use a penetration approach, also knowing which level of vulnerability is acceptable in the system.

70% of people used to see at which level the security must be used, was agreed that it is necessary to have a security plan in every stage of the development life cycle.  
This study shows us that security should be taken into account at each level of a system development stage.