Module 8 Journal

Michael Jones

To begin, there is a very important notion to adopting a secure coding standard within a team, project and company. It is also important to not leave security until the end. Developing a security standard is important within a company because it allows for continuity within the development process. It is important to lay out the ground work for how the team should handle certain situations and mitigate risks of security within the development process for an application. This process needs to be brought forth either at the start of a project or before the project begins in general. This brings upon the point of not leaving security to the end. I believe that it is important to begin handling the issues of security at the beginning of the development process.

Not leaving security until the end is one of the most important things within a project that is often overlooked, or at least drastically undervalued. It seems like every day we are hearing about some company that has been hacked through a very common practice such as SQL injection. A project must begin speaking about security issues at the start of the project and continue discussing changes, optimizations, and maintenance throughout the entire lifecycle of an application.

Companies need to look at evaluations and assess the risks of security mitigation. There will be a cost to any extra processes that need to be implemented. However, I believe that the cost of security is a necessary one.

My recommendation is that we need to adopt and implement a security standard at the beginning of any new project. Also, I believe that there should be a section of the development team that works with the security team and their sole focus is only on security issues. This way security does not get overlooked within any new project.