**CS-405 8-2 Journal: Portfolio Reflection**

**Jason Farrell**

**Southern New Hampshire University**

Regardless of what type of business your application or systems may be fore, you must ensure that they are secured in every way possible. Retail companies especially in which funds are transferred for goods and services. Some vendors who allow you accept payment options also may require certification of your apps and systems to ensure that they also will be protected from any type of incidents that may occur. If people lose trust in your apps and services, your bottom line will also be minimum to what it could be with trusted and secured systems.

This is the need why software apps and services need to have security in mind during the planning and design phases of application development. Waiting till the end when they are already coded could me tons of extra days and refactoring of the apps and services to ensure they are protected in every single way. This refactoring would also include more time regression testing the previous developed features as well. When you include secure application development at the beginning of the software development lifecycle, you’ll find that your development will be more mature and safer than when waiting until the end.

You must also develop playbooks up front that spell out how to handle incident management. Playbooks are detailed written instructions that an incident response team may follow when certain security scenarios arise. The worst time to make up a plan is when some incident is already in action. We must ensure that with proper logging, health and monitor tools are in place so that once an incident happens, we will be notified about it early on when it begins. Some companies also have in place where active monitoring should catch certain incidents before customers can identify and report it to the company themselves. I believe we term this as proactive monitoring.

Today with so many security issues and incidents, we need a zero-trust policy in place. Zero trust builds upon the Triple A ideal in which Authentication (or identity) is proving whom the user really is using the account. It also expands on the idea of authorization in which what rights are granted to which systems, applications and data stores. There are various ways zero trust is implemented in authentication of users in which two factor authentication or even the new Keypass mechanism for determining whom it is really logging into the network and trying to access applications or systems.

Security policies can only be as good as the enforcement of the policies. You cannot have exceptions in any area of the security policies as those would increase the risk of the applications or data exponentially. As stated before, if security is included in the planning and design phase, there shouldn’t be any need of having exceptions on how to bypass certain rules or standards that the security policies put in place.