Reflections on CMGT/400

Nate Bachmeier  
April 26, 2014  
CMGT/400: Information Assurance  
University of Phoenix  
  
Facilitator: Robert Quintin

# Reflections on CMGT/400

## Thoughts on Material

If I knew nothing about security or the surrounding landscape, this would have been an excellent course to learn the broad strokes. This was aligned with my expectations from the title “Core Management Introduction to Info Assurance and Security.” It would have been nice to drill down into more technical aspects, but in all fairness this was an introduction course.

One thing that I did like was that the material aligned with the CISSP book of knowledge. Hopefully this translates to students being able to leverage these 5 weeks during the certification. The *Principals of Computer Security* was also easier to follow than the BOK, especially given the numerous examples of various scenarios and how they are applicable.

## Thoughts on Assignments

My favorite assignment of this course was actually the one I did the worst on. As part of the week 2 Constant Danger paper we needed to determine risk from threats and vulnerabilities. While this was only 10% of the paper, I probably spend 70% of the time thinking of how this section should be computed.

I reused ideas from the Business Fundamentals, Linear Algebra, and Machine Learning to come up with a formula for determining risk priority. The basic idea began with *Risk = Asset Value \* Odds of Failure*.

From there I thought what if there are multiple ways that something could go wrong? If there was failure vectors then the risk formula would need to be rewritten as *Risk = Asset Value \* Sum( Odds of Failure)*.

The problem with this formula is that the odds of risk are dependent on the context. For instance a skilled attacker versus a high school student need to be weighted different. Another example might be environment constraints, such as a bug that is only exploitable during high CPU consumption.

In Machine Learning, we learned that such scenarios are driven by Probability that given a condition set “x” the likelihood that “y” is true is dependent on the context “theta.” This could would mean that the formula would need to be

This was really cool because in this small section of text I was able to combine every course that was running parallel to this into a single fixed thought. The answer made sense and it was submitted.

Then I started to think how about the implementation of that probability function. From some research I discovered Sigmoid functions, which have a property of asymptotes at 0 and 1 and exponential growth toward both extremes. Exactly what I want need!

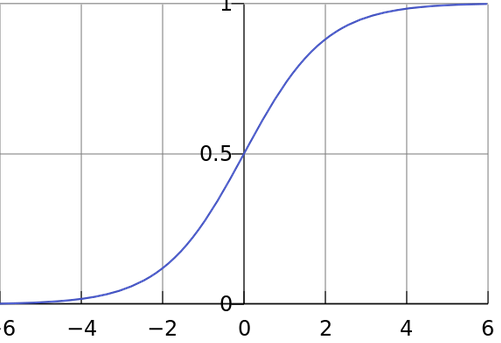


Figure : Sigmoid Function

Now I need to find data sets which provided characteristics of successful exploits; such as did the company patch frequently, firewall policy, data retention lengths, attack surface, etc. Using this information it would be possible to compute theta and actually use this in real life.

## Thoughts on Learning Team

The learning team model at Phoenix is probably the worst thing about this school. The concept is very sound, but it is very easy for it do become derailed and turn into a giant mess quickly.

From experimenting across different courses I believe this comes from two problems; first not using an asynchronous development model, and second the idea of writing 25 pages is scary to many.

By asynchronous, I am referring to a “divide and conquer” strategy which is lock free and everyone is unblocked from the day one until the due date. This can be accomplished by properly segmenting the work among all the people. Typically assignments have natural divide lines such as “describe blah” and “apply blah.” In this example person one gets the first and person two gets the last. At the end of week everyone merges together and you submit.

While this has worked very well in previous classes it did not address the second issue that the big paper was psychologically blocking. In this course I decided to template the weekly papers with the headers and agreed upon task assignments. This way when Joe Bob went to do their section they could approach as just another “simple 250 word DQ.” The rest of the paper was not their responsibility.

This worked incredibly well for our learning team. Everyone knew exactly what was needed from them, the state of everyone else, and there wasn’t any issues in meeting the delivery. We found that interactions between each other was not critical for success, in part due to the lock free divide and conquer system.

Another take away that I got from this is that it works very well, however the overall quality of the paper suffers. The natural flow can be lacking and other editing related work need to be improved. One possible solution might be to rotate a weekly designated editor. More experimentation is required before concluding how to properly solve this problem.