Internship Paper Three

Ashley Myers

CYSE 368 – 33455

Dr. Saltuk B. Karahan

June 21, 2023

As we started getting familiar with the NIST 800-53 Rev 5. I was assigned to do a gap analysis on RA-3(3) Risk Assessment | Dynamic Threat Awareness. The way that this was performed, was that we were supposed to do a risk assessment on Crysallis.AI itself, I will attach the form along with this paper to give an outlook on what the organization was for this gap analysis.

I only heard of the NIST 800-53 Rev. 5 prior to this internship but was not quite sure what it truly was. While serving in the Navy, one of the first things that I learned was to always do all maintenance, inspections and whatever else, ‘by the book’. Learning about the NIST kind of reminded me of what I did in the military. There are so many pubs and references in the Navy that blandly tells one how to perform his or her job. One of the references I used in the military was The Naval Aviation Maintenance Program (NAMP). That reference was the bible on how to perform my job while serving in the military.

By following references, like the NIST or NAMP, if something were to happen, let’s say a mishap, and one did his or her job correctly following the references than that individual has his or her own self covered. The section I had in the NIST was risk assessment. To monitor or determine current and on-going cyber threats to one’s company. In order to have a set of rules within a company for employees to for the safety of the company—risk assessment, security planning policies and procedures, addressing risk, and system security plans must be put in place.

Say that an employee was hired, and he or she read all the policies and procedures, then signed stating they were read and if broken could result in being fired or suspended. In those policies there is a section that states, ‘do not plug personal items into work on computers. Well, the new employee, does not listen and plus his or her phone into the company’s computer, which causes a virus/ security breach withing the companies system. Having NIST 800-53 Rev. 5 in place, the IT and Cybersecurity department will already have a process in places incase this were to occur. The tech department was able to come back from this issue, but the new employee now got fired due to breaking the companies’ policies.

Contingency is very important when having a business and dealing with Information technology and cybersecurity operations. In the short story I have created, the IT and Cyber department were prepared for an attack like this one because of planning and policies set in place. The company might not know when an attack is going to happen, but when it does. They should be prepared for it. In 2019, I was on deployment to South Korea, our server crashed, and we had to go into contingency mode. Normally if something like this happens, it can be fixed quite easily. With limited resources in South Korea, it took four months to be fixed. In this situation, it could have still been prevented because the backup plan fell through and then we were put in a bad place. If the individuals before me prepared this better, it would have not taken that long to be fixed.

To make sure these policies within a company and checking the NIST 800-53 to make sure there were no changes to that, there should be meetings twice a month, to discuss on what needs to be updated, or even reviewed to make sure that the bet plans, and policies are set in place for the company and employees. Technology is only advancing faster than the world would ever think it would, and it is only important to keep patches, polices, firewalls, and everything needed to keep the network and a company’s infrastructure safe from potential cyber threats.

As for the employees there should be planned tests each month to make sure that the employees are aware of what a potential threat is. For an example, have the company send out a fake (phishing) email to see what the percentages are that individuals click on it and or do not. This will help the company know where they stand. Training within a company is also the best way to protect against these kinds of attacks. In the cyber / IT human error is the biggest flaw. Having mandatory training each month and annually for the employees will help minimize these issues.

Having documents that are set to standard to follow are really helpful because it allows a company to have these standards and making sure that things are running efficiently and properly. Without having guidance, laws, regulations. I would be scared to see how things would be ran. It would be a complete mess and most individuals would not care. This also give repercussion to those who do not want to follow the policies that are set into place. NIST 800-53 Rev. 5 is an important section that talks about the guidance of having risk assessment in place within a company.