A Reflection of Experiences

Clifton G. Gibbons

Dept. Information Systems, South University Montgomery

MIS6995: Information Systems Capstone

Dr. Abdullah Alshboul

April 10, 2021

Table of Contents

Introduction

As a young professional in the field of Information Systems and Information Technology, I have gained incredible knowledge and experiences from on-the-job training. These experiences include areas of file transfer networking, FTP service set and managing printing services under various parameters. These experiences have been enhanced by the educational experiences gained through both my undergraduate and graduate studies. This document will share insight into those experiences while sharing my desired expectations for either advancement or new recruitment into this fast-expanding industry.

Targeted Market: Information Security/Cybersecurity Management

Ultimately, my desired role is to work in the industry of Information Security, and more specifically, Cybersecurity. In modern American news, we have seen and experienced cyber attacks from unidentified intruders to government sponsored cyber threats. The most recently know is the Solar Winds intrusion. As a Federal contractor, this company's software was using in government and private organizations alike. It progressed for months before it was detected, and many organizations still are not sure if they were affected or not. Not only is the breach one of the largest in recent memory, but it also comes as a wake-up call for federal cybersecurity efforts (Jibilian & Canales, 2021). For this example, alone, I would enjoy working in this field the most.

The field of Cybersecurity is more than just experience coders being able to detect, analyze and neutralize any particularly threat. There are administrators who work in this field to ascertain the viability of neutralization tools, develop security frameworks and implement security planning which can include Disaster Recovery and Business Continuity strategies. The specialist may be involved in the development of cybersecurity tools based upon his/her experience in the subject matter.

Attributes and Skills Assessment

In the management of information security, it is vital that the individual have a robust and unique set of skills to be highly functional in his/her duties. These skills include communication, analysis and implementation. Additionally, the person has to have reasonable level of integrity to provide confidence to the audience that he/she will be engaging.

Personal Attributes

In providing dialogue with customer/clients/stakeholders, the information security candidate must possess the ability to connect and engage with his/her audience. A sense of both authority and strength mixed with responsibility and restraint must be associated with the individual’s character. These are needed when an incident occurs. Management and staff need to know that they can take charge and facilitate requirements effectively while also accepting responsibility for a failure within their domain and restraining the desire to shift responsibility to others.

Technical/Nontechnical Skills

When it comes to technical experience, a cybersecurity manager has to understand, at least, the building blocks of information security. These include design implementation of security devices (i.e. routers with firewalls, internal/external intrusion detection systems, etc…) and relevant tools to monitor network traffic – something like Wireshark – when a potential threat is detected. However, his/her job becomes more complex when it comes to nontechnical skills.

As a cybersecurity manager, you must be able to effectively translate information from technical jargon into common terms that can be understood by individuals that do not possess the same level of technical expertise. Additionally, you must fully be abreast of all legal, regulatory and industry standards that directly impact the organization's industry. For example, a cybersecurity manager for a hospital must be fully aware of all HIPAA compliance regulations, local laws regarding medical records security and proper implementation of a Cyber Security Framework (CSF). Once such framework can be adopted through the National Institute of Standards in Technology (NIST). Even telecommunications companies will implement framework developments from NIST simply because NIST CSF adoption continues to accelerate as many IT security professionals recognize the framework as a pathway to maintain compliance with regulatory standards, like PCI DSS (AT&T Business). Interpreting and implementing these frameworks while explaining them to a committee of both technical and nontechnical staff requires a unique execution of communication and interpersonal skills.

How South University Has Equipped Me For this Role

While the first part of the paper has reflected on what these positions need/require, I have elected to use terms like he/she or his/her. So, now, here is how I feel that I have been prepared for these role(s). Beginning on my first day of my first class, we discussed the topics of emerging technology and how they will be used in the work place. This topic helped me to determine how security plays a significant role. For example, we discussed the use of biometric authentication. In one of my previous papers, I discussed the power of biometrics likes this:

> "Everything, from passwords to tokens, can be compromised either by server intrusion, weak password integrity, loss/stolen tokens or simple irresponsibility of the user by leaving devices unlocked. For this reason, biometrics become an impressively

> sophisticated means of security because biometric characteristics can neither be stolen nor transferred (Költzsch, 2007).” (Gibbons, 2020).

What I did not realize at the time is how important it would be to safeguard biometric information. If not safeguarded properly, then a breach of privacy could be implicated on the company as a person physical information has been capture, stored and now stolen due to careless security. This would be one of the many rationales I have come to understand through my experiences with South University and, more specifically, the Information Systems Management curriculum. It is these lessons and reasoning skills that will sustain me within the role of any information security (InfoSec) position.

Skills Demonstration

One of the best ways to show that I have insight into the skills for the InfoSec job market involve exercises that have either directly or indirectly prepared me for this position. In this section, I will share some examples that will be applicable to the job role. Remember these are roles are either directly or indirectly appropriate for these positions.

Skill 1 – IT/IS Models (MIS6020: Corporate Information Systems Mgt- Week 3)

Within this course, I and my classmates were challenged to understand the types of device implementations, network modeling and using a modified SWOT analysis. The scope of the discussion followed the migration of services. This is important for my role in InfoSec as it pertains to securing those platforms of service. Understanding a company’s network model will help understand where to pinpoint potential points of intrusion and develop a means of security in those areas.

Skill 2 – Creating Work Breakdown Structures (MIS6010: Project Management – Week 2)

In this project, I was tasked with developing a new worksite project. It was my responsibility to establish what needed to be done, what the budgetary restraints would be, the actors involved, development of communication avenues and production of project reports before, during and after project completion. This is important for my role in InfoSec as it relates to project management of a given department. Whether I start it from scratch, or take over from previous individual, I will need to know how to properly staff and manage the department within the project's scope and budget.

Skill 3 – Creating/Establishing a SETA (MIS6250: Org. Info. Security – Week 3)

The main goal of an InfoSec manager and team is to ensure that the corporate network maintains secured services internally and externally. One of the greatest threats to that security is found inside the corporation: colleagues. Whether intentional or accidental, those you work with are more likely to create security breaches from their actions. By creating a Security Education Training and Awareness platform/framework, the InfoSec team is able to reduce likely breaches cause by internal actors.

Skill 4 – IS Strategic Planning (MIS5020: Information Systems Fundamentals – Week 3)

At the heart of every business, the main goal is to lower cost and maximize profits. As an InfoSec/Cybersecurity Manager, that task will likely be a topic of discussion. "How can you produce the best security with the least number of resources to help maximize profits for the company?" IS Strategic Planning helped to hone those skills for developing actionable game plans to meet the goals of stakeholders, thus preparing me, the manager, how to prepare rationale for acquiring, maintaining or surrendering/removing both equipment and/or personnel.

Skill 5 – Team Building (MBA5001: Organizational Behavior – Week 4)

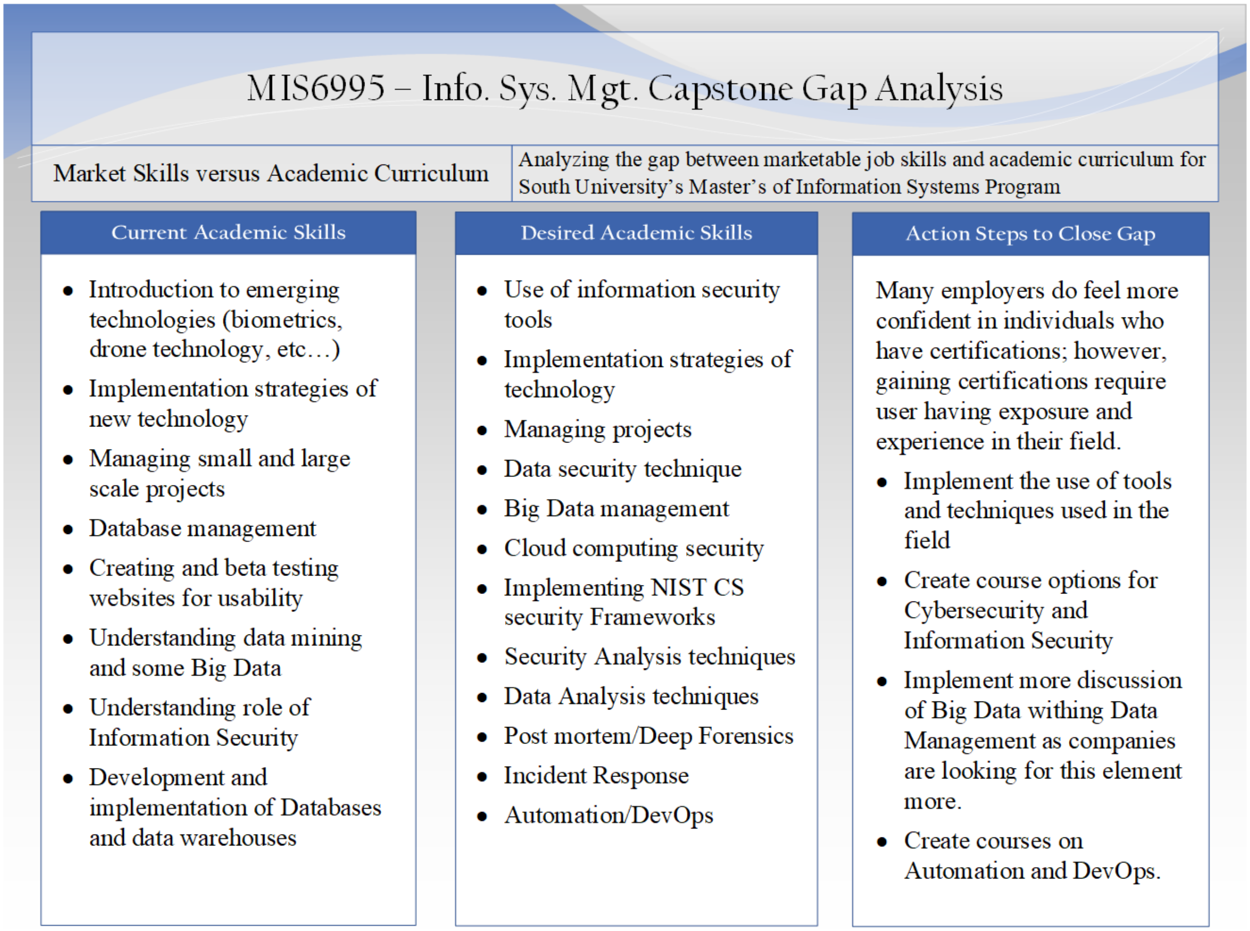
Team building is a useful skill no matter what industry a manager/administrator finds themselves in. While the immediate author of this quote is unknown, the sentiment is incredibly accurate. Gifford Thomas shared his thoughts on the quote that read like this: "A bad manager can take a good staff and destroy it causing the best employees to flee and the remainder to lose all motivation (Thomas, 2019)." As a potential manager, I benefit from this course as it helps to hone my leadership skills and empower those under me through those skills learned and applied.

Job Market Evolution

Technology has evolved and changed since its public boom in the late 1990's. Cybersecurity threats have evolved just as equally. Previously, cybersecurity dealt, primarily, with in-house operations such as installation of antivirus software, management of firewalls and routers and even basic network management such as passwords and email services. That, however, has evolved with the implementation of Cloud-based computing and hybrid networks (cloud and local network services). This evolution has led to the development of Enterprise Cybersecurity Operations (EC-Ops). To remain competitive in this market, one must be ready to address the components of EC-Ops and stay on top of new/developing threats that may target the company/corporation's industry or interests.

Market-to-Education Gap Analysis

Getting the best education to prepare you for your exciting career is the challenge given to every student. There are some that understand this early on in search for the college of their dreams; however, some realize it later on. They may adjust their course of transfer to the school that best serves their interest. South University has, in my opinion, prepared me in unique ways for the position that I desire. Below is a gap analysis I performed on my educational experience and what I think they could do to improve upon what they have already established.



MIS6995 – Info. Sys. Mgt. Capstone Gap Analysis

Market Skills versus Academic Curriculum

Analyzing the gap between marketable job skills and academic curriculum for South University's Master's of Information Systems Program

Current Academic Skills

- Introduction to emerging technologies (biometrics, drone technology, etc…)
- Implementation strategies of new technology
- Managing small and large scale projects
- Database management
- Creating and beta testing websites for usability
- Understanding data mining and some Big Data
- Understanding role of Information Security
- Development and implementation of Databases and data warehouses

Desired Academic Skills

- Use of information security tools
- Implementation strategies of technology
- Managing projects
- Data security technique
- Big Data management
- Cloud computing security
- Implementing NIST CS security Frameworks
- Security Analysis techniques
- Data Analysis techniques
- Post mortem/Deep Forensics
- Incident Response
- Automation/DevOps

Action Steps to Close Gap

Many employers do feel more confident in individuals who have certifications; however, gaining certifications require user having exposure and experience in their field.

- Implement the use of tools and techniques used in the field
- Create course options for Cybersecurity and Information Security
- Implement more discussion of Big Data withing Data Management as companies are looking for this element more.
- Create courses on Automation and DevOps.

Closing

Without reflection, we go blindly on our way, creating more unintended consequences, and failing to achieve anything useful (Wheatley). Reflecting on my experiences at South University, I have learned concepts that changed my reasoning skills in class and on the job. Those changes include my attitude towards management styles, implementation of security for databases and user permissions. I consider what I have learned to be a great honor, and I look forward in utilizing these skills in my professional life and growing those skills to move further within my chosen industry.

References

AT&T Business. (n.d.). *NIST Cybersecurity Framework Compliance with AlienVault USM Anywhere*. https://cybersecurity.att.com/resource-center/solution-briefs/nist-compliance-usm-anywhere

Gibbons, C. G. (2020, February 4). The Rise of Biometrics: An Impact Research of the Benefits, Disadvantages and Security Implications of Biometric Security Software in a Modern Society {Research Paper}. *MIS5030: Emerging Technologies*. South University.

Jibilian, I., & Canales, K. (2021, February 25). *Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal*. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Költzsch, G. (2007). Biometrics - Market Segments and Applications. *Journal of Business Economics and Management, 8*(2), 119-122. doi:https://doi-org.su.idm.oclc.org/10.3846/1611699.2007.9636159

Thomas, G. (2019). *The Inspirational Leader.* Port of Spain - Trinidad and Tobago: Indepedently Published -Leadership First. https://www.leadershipfirst.net/post/a-bad-manager-can-destroy-a-good-staff

Wheatley, M. J. (n.d.). *Reflection Quotes*. Retrieved from BrainyQuote.com: https://www.brainyquote.com/quotes/margaret_j_wheatley_283925?src=t_reflection