Dizon, Arjec Jose A.

BS INFOTECH 3A

IT SECURITY & MANAGEMENT 2

REFLECTION PAPER

When I started the subject *IT Security and Management*, I didn't know much about cybersecurity. All I knew was that it had something to do with protecting computers from hackers. But as the weeks passed, I learned that cybersecurity is a very broad and important field. We started by discussing the cybersecurity challenge how technology is growing, and with it, the risks to our data and privacy. I was surprised to learn how many career paths exist in cybersecurity, such as ethical hacking, security analysis, digital forensics, and more. Each of these roles plays a vital part in keeping information safe. We also discussed the pathway to enter the cybersecurity field, and how information security management fits into the bigger picture of managing IT systems in a secure way. It made me realize that IT security isn't just about using antivirus programs it's about understanding how systems work and how to protect them at every level.

We moved on to frameworks, challenges, and risk management. Here, I discovered that cybersecurity isn't done randomly it follows frameworks like NIST or ISO standards. These frameworks help companies organize their security measures and follow a clear structure. However, even with a good framework, challenges still exist. Cyber threats are always changing, and it's hard to keep up. We also studied the risk management process, which involves identifying risks, assessing them, and planning how to reduce or respond to them. This part of the subject taught me how important it is to prepare before something bad happens. Planning ahead, identifying weaknesses, and knowing the best ways to respond can save a company from big damage. It also helped me understand that security is not about eliminating all risks (which is impossible), but about managing them smartly.

In the next part, we learned about enterprise cybersecurity architecture. This sounds like a complex topic, but it became clear once we broke it down. We looked at "architecture in depth," which means using multiple layers of security, not just one. For example, instead of only having a password, a system might use firewalls, encryption, monitoring tools, and backup systems all at

once. This layered approach is more effective. We also studied the 11 functional areas of cybersecurity architecture, each responsible for different tasks, like access control, monitoring, and risk assessment. We explored incident responses too what steps a company takes when a security problem happens. This taught me that responding quickly and properly is just as important as preventing attacks. It's not just about fixing the system, but also about communicating with users, investigating the cause, and making sure it doesn't happen again.

We also covered how to implement enterprise cybersecurity. This includes understanding how IT organizations are structured and how the cybersecurity life cycle works from planning to maintaining to updating systems. Security policies are also important. These are the written rules and procedures that guide how employees and systems behave. Good policies make sure everyone knows their responsibilities and helps prevent confusion during an emergency. We also talked about selecting security controls, which are the tools and strategies used to protect systems, like antivirus software, firewalls, encryption, and physical security. I found this part helpful because it showed that cybersecurity is not only about digital threats, but also about how people and systems are organized and managed.

In another section, we focused on operating enterprise cybersecurity. This means making sure that the security plan is working on a daily basis. We talked about operational responsibilities what roles people have in maintaining security. It made me see how important teamwork is. For example, one team might handle software updates, while another monitors suspicious activity. Each group must do their job well so that the whole system stays safe. We also discussed IT and cybersecurity processes, like incident detection, response, reporting, and recovery. Understanding these steps helped me see how a company runs its daily operations to stay secure. We also looked at functional area objectives what each part of the organization should focus on to support cybersecurity. Everything has to work together for the system to stay protected.

Another interesting topic was about meeting the cybersecurity challenge. We learned about different types of controls technical, administrative, and physical that help reduce risks. We also talked about security capabilities, like threat detection, response systems, and user education. I realized that technology alone cannot solve security problems. People need to be trained, and policies must be followed. Cybersecurity is not separate from enterprise IT they go hand in hand.

When a company plans its IT strategy, it must also include security at every stage. This is something that many organizations fail to do, and it leads to weaknesses. The integration of IT and cybersecurity is key to creating a safe environment.

We then explored virtualization and mobility. These are very relevant topics today because many people use cloud computing, mobile devices, and work remotely. We learned how cloud computing allows users to store and access data online instead of using local devices. This brings many benefits, but also new risks. Data stored in the cloud must be protected from unauthorized access. We also reviewed enterprise virtualization platforms, where businesses run multiple systems on a single physical server. This is cost-effective but also requires proper management. Mobility and BYOD (Bring Your Own Device) policies were also discussed. Letting employees use their own devices is convenient but can lead to security problems if those devices aren't secure. This part of the course showed me how technology trends change the way we approach security.

Contingency planning and legal topics were also very eye-opening. We learned the importance of business continuity making sure the business can keep running during or after a disaster. Whether it's a cyberattack, a power failure, or a natural disaster, companies must have a plan. We also studied disaster recovery, which focuses on restoring systems and data after an event. Both are important parts of cybersecurity management. Compliance was another topic. Many industries have legal rules they must follow to protect user data, such as GDPR or HIPAA. Failing to follow these rules can lead to big fines and loss of trust. This made me realize that cybersecurity is not just a technical issue but also a legal and business responsibility.

Another key part was the comparison between NOC (Network Operations Center) and SOC (Security Operations Center). The NOC manages the performance and availability of networks, while the SOC focuses on monitoring and responding to security threats. Both are important, and some companies use both. We discussed the benefits and risks of having these centers, such as better monitoring but higher costs. I learned how organizations decide what's best for their size and needs. We also tackled IT project management. This involved planning security projects, setting budgets, and using project methods like Scrum. Scrum was interesting to learn because it's a way of working in small steps and adjusting quickly when things change. It's commonly used in

modern IT teams, and it taught me how important good planning and teamwork are in cybersecurity.

Investigation and remediation were other exciting topics. We looked at the attack lifecycle how an attacker plans, enters, and tries to complete their mission. Knowing this helped me understand how defenders can stop attacks early. We also learned how to respond to incidents how to decide the right steps, inform people, and fix the problems. There are also legal implications, such as when evidence must be collected and used in court. This part made me think about how serious cybersecurity can be. It's not just about fixing a computer it can involve criminal investigations and affect people's lives. We also studied how the Security Operations Center (SOC) works in more detail—control layers, administration, and regular maintenance. It takes a lot of work and coordination to keep everything running safely 24/7.

When we got to implementing IT security management, we studied how to create a security implementation plan. This plan includes setting goals, assigning roles, choosing tools, and creating policies. It helps an organization stay focused and organized in its security efforts. We also talked about the evolving trends in IT security management. Cyber threats change fast, and security must always improve. Companies must review their systems, train their staff, and upgrade their tools regularly. We were taught the steps to take in strengthening IT security management, like auditing systems, updating software, and learning from past incidents. This showed me that cybersecurity is not something you do once and forget. It's a continuous process that needs attention and improvement.

Finally, we discussed types of cybersecurity attacks. These included malware, phishing, ransomware, DDoS attacks, and more. Each attack has different signs and effects. We also talked about hackers and their types white hat (ethical), black hat (criminal), and grey hat (in between). We learned how cybercrime affects people and businesses and how important it is to stay alert. Data encryption was another important topic. It protects information by turning it into a secret code that only authorized users can read. This is one of the strongest ways to keep data safe, especially during online transactions.

Overall, this subject opened my eyes to the wide world of IT security and management. It helped me understand how cybersecurity affects everyone, not just IT professionals. It taught me about the tools, the planning, the teamwork, and the responsibility needed to keep information safe. I feel more prepared now to be part of the digital world, not just as a user, but as someone who understands the value of security and how to manage it. This subject didn’t just teach me theories it taught me lessons that I can apply in real life and maybe in my future job too.