CIDM 6341-70 : Cybersecurity

Q1. Ch#1 [40 points]

a. [10 points] What is CIA? What are Attack Vectors and Payloads?

a. CIA is Confidentiality, Integrity, and Availability

- Confidentiality: Describes what data is available to whom. Usually, one should err on the side of minimal availability of information to ensure the best security. There are several ways that confidentiality can be guaranteed with data systems. Some good examples include implementing a security policy that protects data. These typically will consist of items like security policies for user-level access (as in who holds the keys to open what "vaults" of data). Additionally, a security policy can explain how the data is secured (e.g., utilizing drive encryption and only allowing access via secured SSL connection that requires a two-factor authentication mechanism to open).

  Compartmentalizing data access is also another way of ensuring confidentiality. Compartmentalizing is related to user-level access but goes one degree further by placing access controls across multiple areas. For example, you may have basic access to a database with aggregate sales figures for forecasting; however, the source data is restricted to finance users who need the data to invoice clients. Thus, the sales user does not have access to the source data compartment.

- Integrity: This describes how complete a set of data is. Data corruption can happen via many different methods, including impending drive failure, transmission errors, malicious activities (e.g., virus, ransomware). Ensuring data integrity is essential since incomplete or corrupted data is worthless.

- Availability: This describes if the appropriate data or systems are available to users authorized to have access. For example, if you have a managed network drive, they should have easy access to the stored data after a user authenticates. Another example would be a database that contains information that is needed. It should be accessible via some predetermined mechanism (e.g., BI software like Tableau)

b. Attack vectors and Payloads

- Attack Vector: An attack vector is a mechanism utilized to conduct an attack. For example, a human means to do the same (e.g., phishing to get network credentials, getting someone to install a virus that enables a bad actor to gain a foothold). Another good example is a virus being used as a vector to install ransomware on a network.

- Payload: This term is generally used to describe something that is delivered. For example, a payload could be used to describe what a packet is carrying over the

internet. It can also represent malicious code that is installed on a victim's machine.

b. [20 points] Assume that a security model is needed to protect information for an elder care information management system. Use the CNSS model to identify each of the 27 cells needed for complete information protection. Write a brief statement that explains how you would address the components represented in each of the 27 cells.

    a. Confidentiality: Restrict information related to patient treatment to only those identified as treating a specific patient. Access to patient's records should only be granted by a third-party agent that can verify that the person requesting the data will be treating the patient in question (e.g., by a care coordinator assigning a patient to a treatment team. Patient's guardians could have access provided via registration with care homes patient portal, which requires patients to have a specific access code to begin the registration process. That access code will need the guardian to verify the patient's identity by providing data during check-in (e.g., Social Security Number, Date of Birth, etc). They would also need to provide proof that they have power of attorney.

    b. Integrity: All treatment staff is needed to have a badge displayed prominently on their person. This badge should have a photo and indicate their role (e.g., Registered Nurse). These badges should allow the individual into secure areas that require badged access. Additionally, they could be used as an additional second-factor authentication security mechanism when accessing a system.

    c. Availability: Patient data shall be available to the treating staff with controls stated above. Data should also be available to patient's guardians on-demand via a patient portal that requires registration. The data should be easy for both clinical staff and guardians to access securely.

    d. Confidentiality—Policy—Storage: Patient data shall be stored in the secure electronic record management system. All data shall be stored in a secure data center that is PCI Type II compliant This data must be encrypted on the drive to prevent unauthorized access should malicious parties obtain access to the physical drives. Additionally, mass data with PII (personally identifiable information) shall not be exportable. The data may be exported on an individual basis if the individual has specific permission to do so (e.g., a patient or guardian's consent to share the data with care providers).

    e. Confidentiality—Policy—Processing: All data access to clinical staff will be provided by a separate entity (e.g., care coordinator) to add a layer of security before giving access to the data to a clinician. Patients or their guardians must fill out questionnaires via a secure portal before admission or via a secure tablet with the data provided directly to the electronic records management system. Two-factor authentication will be required for all authentication methods. Secure passwords must also be used with a minimum of 12 characters, a mix of upper and lower case, numerals, and symbols. Additionally, utilize a password history to prevent re-use of the last 12 passwords.

f. Confidentiality—Policy—Transmission: All patient data should be transmitted to the secured electronic records management system utilizing SSL encryption protocols (https). The only way data can be accessed internally via wireless networks is when accessed from specific IP ranges assigned to secured access points utilizing WPA2 or greater.

g. Confidentiality—Education—Storage: Provide training to staff via the learning management system to instruct them on how to access confidential patient information and how to safeguard it. Additionally, provide patient's guardians with educational material on how to access their data via the patient portal.

h. Confidentiality—Education—Processing: Provide training to staff via the learning management system to instruct them on how access is granted to the clinician. Educate patient's guardians on how their data is going to be safely processed via secure methods.

i. Confidentiality—Education—Transmission: Instruct staff with training via the learning management system to instruct them on how data is secured during transmission and how they will need to utilize credentials to authenticate that they do have access. Patients will be forced to use https when browsing the patient portal by re-directing them if they attempt to go to http instead.

j. Confidentiality—Technology—Storage: All data shall be stored in a secure data center that is PCI Type II compliant All drives shall utilize at least 256-bit encryption. All workstations will be equipped with a reader who will read the user's badge and use it as a second-factor authentication method. When the user wishes to leave the workstation, it will automatically log out when the badge is removed. Patient's guardians will be required to set up a second-factor authentication using an authenticator app or SMS messaging (strong encouragement to use an authenticator app vs. SMS due to SMS's relative ease of hijacking).

k. Confidentiality—Technology—Processing: All clinicians will require password authentication with an additional second-factor authentication using their work badge. Patient's guardians will be required to use a secure tablet or patient portal.

l. Confidentiality—Technology—Transmission: All data shall be transferred via https and require authentication of identity.

m. Integrity—Policy—Storage: Only individuals with appropriate permission may modify patient data. Data should only be modifiable by appropriate staff members (e.g., care coordinator can add or change insurance information, but clinicians can enter patient's vitals). The patient's guardian should have access to change certain aspects via the portal (e.g., address, medications, allergies).

n. Integrity—Policy—Processing: Data shall be hashed to be error-checked before being committed.

o. Integrity—Policy—Transmission: Data shall be encrypted and have the keys checked to ensure that man in the middle attacks have not occurred.

p. Integrity—Education—Storage: During training sessions about data entry, different roles will be educated on adjusting appropriate data. Additional information will be provided to ensure that staff understands who can change which data.

q. Integrity—Education—Processing: Ensure that staff is trained not to improperly input information (e.g., adding patient's vital statistics in a notes area).

r. Integrity—Education—Transmission: Staff should be instructed on how to effectively input data into the system and ensuring that it has been sent and received correctly.

s. Integrity—Technology—Storage: All data should be stored so that authorized individuals can only change it. Backups should be made to ensure data loss does not occur if a catastrophic device failure occurs.

t. Integrity—Technology—Processing: Utilize data hashing to ensure that the data has been received intact and uncorrupted.

u. Integrity—Technology—Transmission: Confirm the data input to ensure that it was recorded correctly.

v. Availability—Policy—Storage: Data shall be accessible via authenticated means which are restricted to the appropriate level based on the individual user accessing information

w. Availability—Policy—Processing: Authentication shall ensure that data is processed by individuals who have been provided with the proper permissions.

x. Availability—Policy—Transmission: Only authenticated users are allowed to access data via secure web communications.

y. Availability—Education—Storage: Staff should be instructed on the appropriate location (e.g., don't store patient vitals in an excel spreadsheet, keep it in the electronic records management system in the vitals area under the patient's care record).

z. Availability—Education—Processing: Provide training that instructs users on how to input data so that everyone can interpret the data (e.g., use metric measurements everywhere when working with patient vitals).

aa. Availability—Education—Transmission: Educate staff on ways to ensure that their systems remain uncompromised so they can securely transmit patient data.

bb. Availability—Technology—Storage: Data should be encrypted and have redundancy to minimize data loss. Utilizing RAID mirroring and real-time backups will ensure that data is available. Additionally, patient's guardians would need to register to access their data securely. Staff should have their access centrally controlled so their ability to access the data can be enhanced.

cc. Availability—Technology—Processing: Data should be available via the patient portal or electronic records management system.

dd. Availability—Technology—Transmission: Users should have the ability to access data they are entitled to securely.

c. [10 points] What is Cyber-attack? How does an organization protect against ransomware attack?

a. Cyber Attack: A cyber attack could be described as an attack that comes externally from "Cyberspace." Typical examples of this would be black hat hackers attempting to breach a network or server. They could also use human means to do the same (e.g., phishing to get network credentials, getting someone to install a virus that enables a bad actor to gain a foothold).

b. Ransomware attack:

a. What it is: This is malicious software that is installed on a computer system that encrypts the drive contents. The user is prompted to pay a ransom (usually in bitcoin) to decrypt the drive.

b. How to protect against it: There are several ways to protect against ransomware. One important strategy is to have data backed up and tested frequently. Multiple copies of backed-up data should be available (possibly going back months) if the malware was not caught until much later. Cloud-based backups can be helpful since, many times, their own systems have additional layers of protection implemented. Utilize a layered approach to data security. For example, web servers should live in a DMZ in front of the firewall, while database servers should be behind firewalls. Servers should be on different "networks" (e.g., VLANS), which can help stop the propagation of many worms since they look for items on the same network to propagate. Cloud-based systems also help. Install robust (and updated) malware protection that should help identify known malware strains before they can infect the system. Restrict users to minimal levels of access on the network and computers. If the user cannot install the software, it is much more difficult to infect; even if one user is compromised, it is much more difficult for an entire network to get infected.

Q2. Ch#2: [40 points]

a. [10 points] What is a policy differ from a law? Briefly explain the breach law.
    a. "Policy" describes acceptable behavior or standards that an organization defines. The primary difference between law and policy is that ignorance of the law is not defensible; however, ignorance of a policy is (which is why we are always asked to acknowledge that we have read a policy before doing certain things).
    b. Breach laws dictate the actions that a company must undertake after a breach has occurred, resulting in loss of data. This data can vary but usually involves PII (personally identifiable information) of some sort. Many laws require that a company provide post-breach support (e.g., credit monitoring for one year). There is currently no national breach law; however, all states have some sort of breach notification laws.
b. [20 points] Briefly explain the following (ANY TWO) Professional Organizations' Codes of Conduct"
    a. ACM (Association for Computing Machinery): This association was established in 1947 and is the "world's first educational and scientific computing society." They promote education (and provide students with discounted memberships). They have several publications on a variety of subjects related to computing. The code of ethics that their organization has adopted encourages their members to "perform their duties in a manner befitting an ethical computing professional." Some specific areas covered include:
        i. Protect the confidentiality of information (which is the point of Information Security)
        ii. Do no harm (they specifically call out viruses)
        iii. Protect others privacy (goes with the first point)
        iv. Respect others copyrighted material and intellectual property (meaning, don't steal or represent someone else's work as your own)
    b. $(ICS)^2$(International Information Systems Security Certification Consortium): A non-profit whose primary focus is on developing and implementing credentials and certification for InfoSec professionals. They maintain a wealth of information about InfoSec and provide training, and provides certification examinations. They have a code of ethics that they want their certified professionals to follow. This will help guide InfoSec professionals on being trustworthy and ethical stewards of the profession. Their code includes the following four being the mandatory canons:
        i. "Protect society, the common good, necessary public trust and confidence, and the infrastructure."
            1. This means that individuals should strive to work for the betterment of their fellows and provide protection for infrastructure. To be a good InfoSec technician, you have to think like your adversaries, and the Darkside is tempting.
        ii. "Act honorably, honestly, justly, responsibly, and legally."
            1. This means that individuals should be proud of themselves if everyone knows their acts.
        iii. "Provide diligent and competent service to principals."

1. Meaning that the principal (I'm assuming that they mean clients) should be provided with thorough and good work.

iv. "Advance and protect the profession."

1. This means that one should do their best to better the profession and protect it from damage.

c. [10 points] What are steps in a digital forensic process, and when is it used in a business setting?

a. Digital forensics describes a methodology used to identify the root cause of an incident when the event happened to a digital system. Some examples of how it might be used in a business setting could include understanding how a security breach occurred, the cause of a service outage, policy violations, lawsuit discovery. The methodology usually includes the following steps:

i. Identify items of evidentiary value: Meaning identify something that is likely to be used to track back to misconduct.

ii. Acquire evidence without damage or alteration: Meaning don't contaminate it, which would make it unusable in court (fruit of the poisonous tree, many people have "gotten away with it" because of mishandled evidence)

iii. Ensure that proper steps are taken with the evidence at every stage to guarantee its authenticity and that it has remained unaltered: This means to establish a chain of custody, so the authenticity of the evidence won't be called into question.

iv. Conduct any analysis without risking unauthorized access or modification: This means that the use of copies to conduct analysis. Additionally, the evidence should be protected from unauthorized access (e.g., encrypted or kept in a physically secured manner under lock and key)

v. Any findings of illicit activities should be reported to proper authorities: Pretty much speaks for itself. Evidence of a crime should be reported to the proper authorities

Q3. Ch#3: [40 points]

a. [10 points] What is security planning? What are the three common levels of planning?
    a. Security planning is how one sets a specific goal to be accomplished, the time allocated to achieve it, and any steps that need to be done. For example, a strategic objective could be proactively addressing attacks. As the first step in Q2, we need to have an intrusion monitor system identified and proof-of-concept operating.

       Organizations determine if planning is needed based on weighing the benefits of a security planning effort versus its cost.
    b. Three common types of planning include Operational (coordination of activities between different segments of the business), Strategic (Long-term for the organization as a whole), and tactical (shorter term, usually a piece needed in accomplishing a strategic plan).
b. [20 points] Briefly explain CERT Governing for Enterprise Security Implementation with the framework.
    a. This framework was published by Carnegie Mellon University and developed by Jody Westby and Julia Allen. It provides some excellent insights into what needs to be done to develop and support InfoSec governance. The framework stipulates that a Board Risk Committee (BRC) will drive the Enterprise Security Program (ESP) for an organization alongside stakeholders and senior leadership. The program should enable an organization's ESP efforts to function (e.g., risk management programs). The GES (Governing for Enterprise Security) program should incorporate three articles:
        i. Characteristics of Effective Security Governance: This document focuses on defining what effective security governance should look like. There are eleven characteristics:
            1. InfoSec affects everyone and everything within an organization
            2. Leaders are not alone for InfoSec accountability; the business environment, stakeholders, and their communities are all accountable
            3. InfoSec is a business requirement that must be aligned with the organization's overall strategic goals
            4. ESP needs to be based on risk and have a risk management program
            5. Roles in the ESP should be well defined "de-conflicted' to avoid conflicts of interest
            6. Requirements for ESP should be specific and enforceable via policies and procedures
            7. Appropriate and adequate resources should be provided for the ESP
            8. A Security Education, Training, and Awareness (SETA) program should be created and enforced across the enterprise
            9. Information security should be integrated throughout the life cycle of all software and systems implemented by the organization
            10. Well monitored and maintained metrics should be defined for the ESP
            11. The BRC should periodically audit the ESP to ensure that their goals and objectives are aligned with the organization
        ii. Defining an Effective Enterprise Security Program: This document creates the methodology for creating and maintaining the ESP throughout the organization. Additionally, it defines how the BRC should be composed and what their

responsibilities should entail. A hierarchy of programs is defined as a pyramid with "Risk Management" at the top, "Enterprise Security Strategy" next, "Enterprise Security Plan" after that, and ending with the "Business Units." The BRC is responsible for:

1. Establishing an organizational ESP structure
2. Top-level policies and actions should be used to "set the tone" for risk management within an organization
3. Suitably qualified individuals are placed in for the creation and maintenance of the ESP as well as keeping them trained
4. Creating roles and responsibilities that are de-conflicted by segregating duties
5. Getting a security budget approved by the board and allocating monetary resources based on security needs and ROI
6. Having risk assessments conducted and reviewing their results as well as conducting periodic reviews of the ESP
7. Managing the risk management program, enterprise security services and enterprise security plan, disaster recovery, incident response, crisis management for the organization
8. Monitoring and mitigating any weaknesses in the ESP and ensuring it is up to date

iii. Enterprise Security Governance Activities: This document establishes the finer details of the ESP and GES. The roles and responsibilities of the executive management team and the BRC are defined. Additionally, there is an establishment of a governance structure that incorporates a reporting framework, roles and responsibilities, and some of the needed high-level policies. This ensures that the BRC can ensure that security operations are monitored and maintained to ensure they are kept up to date.

c. [10 points] Compare managerial, operational, and technical security controls? Why is maintenance needed for information security management systems?

a. Managerial Control: Are implemented by security administrators based on security processes designed by strategic planners for an organization. They address the design and implementation planning process. Additionally, they address ongoing security reviews and risk management. Finally, they also address the maintenance and legal compliance of the security system as a whole.
b. Operational Control: This is the management of lower-level planning and functions (e.g., disaster recovery). They usually also address various aspects of security (such as personal or production inputs and outputs). The ongoing education of employees and managing maintenance and data integrity can also be included.
c. Technical Security Control: These items must be made or purchased and then integrated into the overall infrastructure for an organization. Additionally, items included here are logical controls used for identification, authentication, authorization, and accountability.
d. Maintenance is needed for infosec management systems because threats are constantly evolving and must be addressed systematically. Maintenance is the most crucial phase in the

SecSDLC because remaining static is a sure way to ensure that systems will have vulnerabilities that can be exploited.

Q4. Ch#4: [40 points]

a. [10 points] Briefly explain spheres of security in terms of use and protection.
    a. An information security policy is the collection of policies created by an organization. These policies help ensure that users within the organization follow the guidelines and rules placed to ensure the security of information. The sphere of security shows how people are involved in policy and law regarding information, systems, networks, and the internet. It also shows how technology (especially access controls) is provided across most of the layers as well. Security planning is also outlined in the people side of the equation.

b. [20 points] To produce a complete information security policy, management must define three types of information security policies: (i) Enterprise information security program policy, (ii)Issue-specific information security policies, and (iii) Systems-specific policies. Compare these three policies. [Hints : one approach of answering can be creating a table comparing these three policies].
    a. The following table makes a comparison. Where colors match for EISP and ISSP, those indicate where the categories line up most closely. In the SysSPs column, it outlines which group the ISSP would likely fall into

EISP	ISSP	SysSPs
Protection of Information	Statement of Purpose	Managerial
Use of Information	Authorized Uses	Managerial/Technical
Information Handling/Access/Usage	Prohibited Uses	Managerial/Technical
Data & Program Damage Disclaimers	Systems Management	Technical
Legal Conflicts	Violations of Policy	Managerial/Technical
Exceptions to Policies	Policy Review & Modification	Managerial
Policy Nonenforcement	Limitations & Liabilities	Managerial
Violation of Law		
Revocation of Access Privileges		
Industry-Specific InfoSec Standards		
Use of InfoSec Policies & Procedures		

    b. Beyond the basic comparison of the above, EISP could be defined as the broad policies, and the ISSP is the standard by which the policies are applied. That is why there are overlapping colors to indicate where they (generally) line up together. Some spots could overlap (e.g., "violation of law" could also fall under "prohibited use", "exceptions to polices" could fall under "policy review and modification," and "limitations and liabilities"). The SysSP defines the system-specific policies that are broadly broken into a managerial or technical grouping. I tried to indicate where they would fall more under for each of the ISSP categories. For example, with authorized uses and prohibited, a policy could be created, and the technical side has to enforce by use of ACL.

c. [10 points] What do you mean by Access Control Lists? Give an example.

a. ACL is the access control list. In a nutshell, it dictates what you can do within an operating system. In Linux, secure access to information is done by assigning "groups" to folders. The group that is defined in the folder can have specific rights (e.g., read, write, execute). Access to all others can be set as well. Groups can be added to specific users to grant them special access to specific directories. The root user and users with sudo access have access to all files regardless of ownership (there is only one root, but equivalent access can be provided via sudo access). If "root" access is needed, the user should be added to the sudo group. Using the sudo command, one can execute commands as root. Logging in as root is not a good practice in general because it's very easy to cause damage to the system accidentally. It's also recommended to disable SSH access to the root user to prevent intruders from trying brute force attacks to gain entry.

Q5 : Ch#5 : [40 points]

a. [10 points] How can you distinguish the cybersecurity in large vs. small organizations?
    a. Smaller organizations typically have a larger percentage of their budget allocated for cybersecurity because their size is smaller. Smaller organizations also usually have a less structured approach but are able to adapt more quickly—think of a small dinghy's maneuverability vs. a large yacht. The larger you become, the longer it takes to change directions; however, once you do, there is a lot more "oomph" available to move forward. You will typically find one full-time individual responsible for cybersecurity and possibly 1-3 part-timers to help out with the systems in a small organization. There are usually more formal policies and controls in a larger organization, and they typically need more staff to manage their needs. You will likely see 1 – 2 full-time managers, 3 – 4 part-time. From a systems perspective, one might find 3 – 4 full-timers and 10 – 12 part-timers.
b. [20 points] Given the structure of an organization, extend it with a cybersecurity department. Briefly explain your choice.
    a. A graphic has been placed on the last page based on the original org chart provided for this question. An InfoSec committee was added under the board of directors because there have been many cases where it was important to have policy generated from an organizational level, and the board is best able to direct that. I then added a CISO (which could have been the cybersecurity department). There's a dotted line connecting that individual role with the InfoSec committee because there must be a direct line to ensure that the directives are being communicated and reported upon as clearly as possible. With Security garbling things second or third hand can be disastrous. This configuration also helps "Open the purse strings" by cutting out the middleman since the board can often have discretion about where to fund things when the budgets are approved. The CISO also reports to the CEO directly. The CISCO and committee would work on the EISPs.

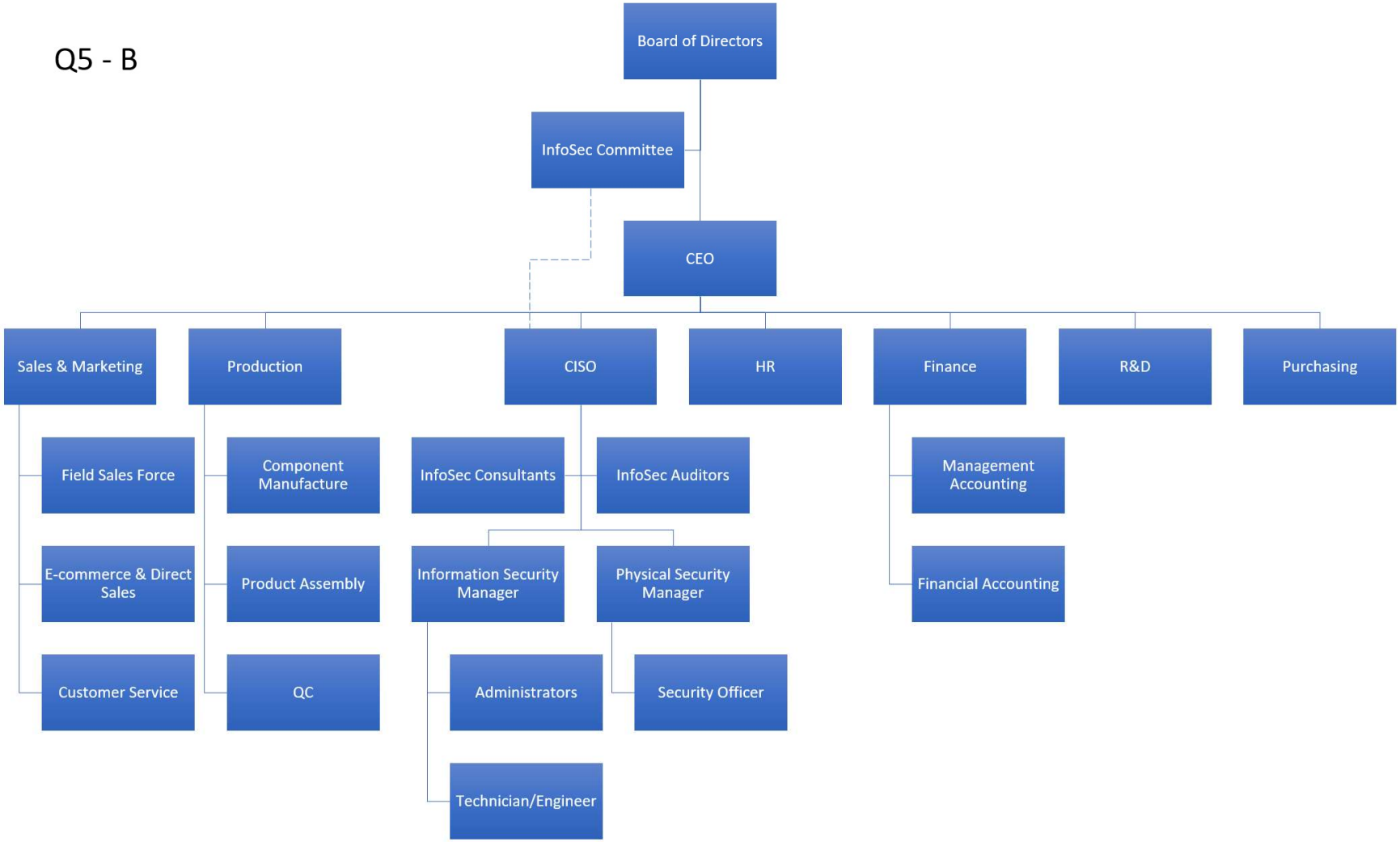
       I added two direct reports (should have been dotted, but I couldn't figure out how to do it with PowerPoint) for auditors and consultants. Consultants are needed to help with things like penetration testing and such. External auditors would also be essential as well to ensure that policy is being followed (My quarterly torture is meeting with the auditors, and it's coming up soon). Then I used the general outline that you had provided in the slide deck for the actual makeup of the department with an IS manager and PS manager. The IS manager would be lead on implementing policy (ISSPs translated from the EISP), continuous improvement, and day-to-day operations. It could probably be broken into several managers who focus on those parts individually in a large organization. There are administrators and technicians or engineers that report to the IS manager. They would be responsible for the day-to-day operations of keeping the lights on and implementing new technology as needed. They would also take the SysSPs translated from the ISSPs and make them happen.
c. [10 points] What is SETA program? How can we implement a SETA in our organization?
    a. SETA is Security Education, Training, and Awareness. This is the process by which all users are brought into the security world and provided with the knowledge that they, too, are a part of the InfoSec landscape. They are in fact the first line of defense because the

human factor is oftentimes the factor that gives bad actors the ability to get a foothold into an organization. Technological exploits are a risk; however, the human element is often the most exploitable of them all. It takes only one bone head mistake to bring an entire organization to its knees (ransomware attacks are a perfect example of this). A good SETA program is key to protecting an organization's security.

b. SETA can be implemented via many directions. Live training can be conducted (my company has yearly ones that are actually kind of fun). A framework would be something along these lines:

	Awareness	Training	Education
Attribute	Teaches users what security is and how they should react in certain situations (e.g., suspicious email from the "CEO")	Teaches users how to respond when a threat is encountered under different circumstances	Purveys why the organization reacts in a way
Level	Basic information about the types of threats and responses	Purvey knowledge about detecting and reacting to threats	Provides a breadth of insight on how and why processes and policies are developed and maintained
Objective	Recognition of threats and ways to respond to them (e.g., forward the suspicious email to the security team)	Users can respond using learned skills	Utilizing an understanding of knowledge gained, an active defense can be mounted and continuous improvement can be made
Teaching Methods	Videos Posters (Only you can prevent system outages)	Formal training Hands-on practice	Theory instruction Discussions and seminars
Assessment	Simple tests that ensures the user was paying attention	Problem Solving	Essay
Impact Timeframe	Short-term	Intermediate	Long-term

Q5 - B


Board of Directors
InfoSec Committee
CEO
Sales & Marketing
Production
CISO
HR
Finance
R&D
Purchasing
Field Sales Force
E-commerce & Direct Sales
Customer Service
Component Manufacture
Product Assembly
QC
InfoSec Consultants
InfoSec Auditors
Information Security Manager
Physical Security Manager
Administrators
Security Officer
Technician/Engineer
Management Accounting
Financial Accounting