FACULTY OF COMMERCE
BIS PROGRAM

Information Systems Security (BIS 405)

Monday, 21th May 2018
02:00pm – 05:00pm

EXAMINATION INSTRUCTIONS:

- Students are not allowed to use calculators.
- Do not use highlighters on your answer booklet.

QUESTION 1 – 30 minutes (9 Marks)

Please, indicate your opinion about the following using the scale below (Justify your answers):
0 = unacceptable, 1= minimal security, 2=acceptable, 3= effective, 4=recommended

	Bank	**Grocery Store**	**University**
Packet filtering firewall			
Application-level firewall			
Hybrid firewall			

QUESTION 2 – 60 minutes (15 Marks)

Give your opinion about the following statements and justify your answer:

1- While many IT professionals may think they would be better off in the big IT departments of reputable organizations, they may in fact be better off at a smaller organization (Maximum **Two** page).

2- If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology (Maximum **Two** pages).

3- While CISOs sometimes claim that the performance of InfoSec is almost impossible to measure, in fact they are measurable (Maximum **Two** pages).

… CONTINUED OVERLEAF

QUESTION 3 – 20 minutes (6 Marks)

The following is a SWOT analysis for security strategy:

Strengths	Weaknesses
- New security leader is highly experienced - Lack of security awareness program - Strong company culture on being compliant with policies	- Lack of security policies on handling company information - Cloud provider has additional services for protecting customer data - Cloud providers are regionally located in an earthquake zone
Opportunities	**Threats**
- Security training that can be bought "off the shelf" will meet company needs. - Discounted protection software available for devices - Employees are buying a wide variety of laptops	- Financial services are targeted by advanced, sophisticated threats. - Lack of supply of experienced information security staff. - Employees are general IT experts

Required:

Find the errors in the above figure?

QUESTION 4 – 40 minutes (10 Marks)

Company X is going to hire a security manager. The CISO reviewed the applications. There should have been many more than just three applications for the position. The CISO called the HR manager.

The CISO: "I'm worried about the number of applicants we have had. I really thought there would be more than three."
The HR manager: "Oh, there were dozens, but I pre-screened them for you."
The CISO: "What do you mean? Pre-screened how?"
The HR manager: "Well, we pass on only the most qualified applicants. According to our criteria, applicants for information security positions must have a CISA certification or some level of GIAD."
The CISO: "Since I am not aware of such a certification as a 'GIAD', you must mean 'GIAC'."
The HR manager: "No the file says GIAD"
The CISO: "Well, for this position we need a CISSP or CISM, not a GIAC or CISA. Those certifications don't match the job description I wrote, and I don't remember specifying any required certifications.

… CONTINUED OVERLEAF

The HR manager: "You don't have to. We have determined that the best people for the jobs are the ones who have the most certifications. We rewrote your position's screening criteria. We don't really look at anyone who isn't properly certified. Is there a problem?"

Answer the following:

1- If you were the CISO, how would you reply to the HR manager's question?
2- What, if anything, is wrong with the human resources focus depicted here? Do certifications alone identify the job candidates with the most appropriate expertise?

QUESTION 5 – 30 minutes (10 Marks)

Match each of the statements below with its proper term.

a) Role based access controls	1) It allows the system administrator to set up accounts that will allow each user to have full access to the files and resources needed, but no access to other information and resources.
b) Identification Mechanism	2) Delivery person shows his ID to the security staff
c) Firewall	3) The top information security staff in the organization
d) Chief Information Security Officer	4) Determine whether the authenticated entity is permitted to access a system
e) Security manager	5) With this configuration, the proxy server is exposed to the outside world
f) Application-level firewalls	6) The administrator assigns the associated access rights to the role.
g) Discretionary access controls	7) Individuals, who configure firewalls, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technology is properly implemented.
h) Packet filtering firewall	8) A mechanism that can prevent the dangers of internet from spreading into a LAN.
i) Authorization	9) Limiting access to information such as gates and alarms
j) Administrative controls	10) Individual users may determine the access controls
k) Subject	
l) Mandatory access controls	
m) Security Technicians	
n) Physical access controls	
o) Authentication	

End of the Exam

Good Luck ☺

… CONTINUED OVERLEAF