Exam Cybersecurity Management

28 January 2016

Weight of the questions

Part 1	Each question 5 points
Part 2	Each question 10 points
Part 3	Each question 10 points

Grade = round(total / 20)

Part 1 – Multiple Choice

Each question has only one correct answer.

Q1 – What are the key concepts that describe cyber security governance?	Answer
a. Risk management, threat intelligence and IT security	
b. Governance of data	
c. Response and Elimination	
d. Direction and reporting	

Q2 – Who is accountable for proper cyber security governance?	Answer
a. The board of directors and senior management	
b. The information security officer	
c. The database owner	
d. The government	

Q3 – What advantage does the availability of relevant data provide?	Answer
a. Enabling analytics and calculations in the cyber risk model	
b. Measuring the performance of the cyber security function	
c. Calibrating the assumptions and parameters in the model	
d. Reducing the uncertainty component of cyber risk	

Q4 – What are conceptual elements of Identity and Access Management?	Answer
a. Access enforcement and login control	
b. Roles and responsibilities, principles and policies	
c. Identity management, authentication methods and authorizations	
d. Single sign-on and account management self service	

Q5 – What is the difference between identification and authentication?	Answer
a. Identification is stating your identity, authentication is providing some proof of your identity	
b. Identification is reviewing someone's passport at the gate, authentication is allowing someone access to the building	
c. Identification is the list of possible threats, authentication is the validity of the information provided	
d. Identification is described in the information security policy, whereas authentication is an element of information security standards	

Q6 – Of the following properties, which is considered most important in industrial control settings?	Answer
a. Confidentiality	
b. Integrity	
c. Availability	
d. Safety	
e. Non-repudiation	

Q7 – In which of the following levels of the ISA-95 model would a Manufacturing Execution System typically be categorized?	Answer
a. Level 4 (Business planning and logistics)	
b. Level 3 (Operations management)	
c. Level 2 (Supervisory control)	
d. Level 1 (Basic control/process control)	
e. Level 0 (Sensors and actuators)	

Q8 – You are asked to hack the mailbox of a CEO. What would yield the most success?	Answer
a. Hack the computer network and identify the CEO's device (iPad, laptop, etc.)	
b. Start a phishing campaign targeting the IT department	
c. Walk inside the office and steal their iPad	
d. Call the CEO directly and social engineer him into giving access	
e. Attempt all of the above	

Q9 – What is Open Source Intelligence?	Answer
a. Security review of Open Source software	
b. Information available in an Open Source/Copyleft format (e.g. Creative Commons licensing)	
c. Intelligence collected from publicly available sources	
d. Intelligence collected from hacked organisations and in particular hacked Open Source databases (MySQL, etc.)	
e. All of the above	

Q10 – Which of the below is part of the security monitoring process?	Answer
a. Collecting events (logs)	
b. Adding business and threat context to events	
c. Normalizing and analysing events (logs)	
d. Gathering security insight	
e. All of the above	

Q11 – Which role would you not expect in a Security Operations Center (SOC)?	Answer
a. SOC engineer	
b. L2 security analyst	
c. Windows Administrator	
d. SOC manager	
e. I expect all above roles in a SOC	

Q12 – Which of these is not a building block in crisis management?	Answer
a. Structure	
b. Governance	
c. Plan	
d. Decision making	
e. Intelligence	

Q13 – What is the main outcome of the Determine Actions activity from Crisis management decision making process (CMDMP)?	Answer
a. The activity is not part of CMDMP	
b. List of activities	
c. List of who does what	
d. List of actions with priorities	
e. Validated course of action	

Q14 – Testing your incident response plan is part of which of the NIST phases?	Answer
a. Preparation	
b. Detection and analysis	
c. Containment, eradication and recovery	
d. Post-incident activity	
e. Can be applied during every phase	

Q15– Which of the following steps is not part of the 3-step 'breach triad'?	Answer
a. Infiltration	
b. Multiplication	
c. Exfiltration	
d. Aggregation	
e. None of the above are part of the triad	

Part 2 – Content Questions

1. Why do you use a framework when defining and realizing cyber security governance?

2. Name at least 5 of the 7 main components of the conceptual cyber risk quantification model and their purpose:

3. Describe the concepts of *business roles* and *IT roles* in Identity and Access Management and their uses; discuss the relationship between them.

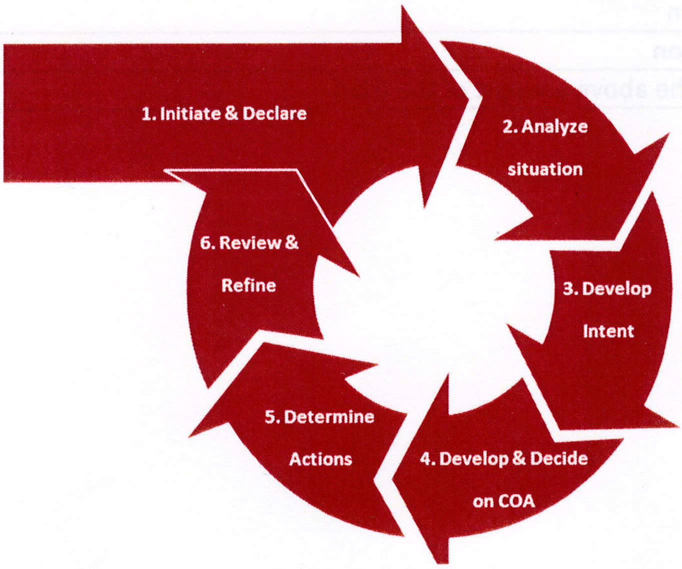
4. In a typical situation, how do IT and OT systems differ in terms of life cycle length, and how does this reflect upon the security measures needed to secure the environment in SCADA settings?

5. When is the right time to do Open Source Intelligence and overall reconnaissance?

6. In order to make sure that a Security Operations Center focusses on the most important threats, scenario analysis and use case engineering are very important processes. Describe 5 key steps in these processes in chronological order.

7. What are the considerations when conducting a volatile (live) data capture and analysis?

8. Describe the Crisis management decision making process. Explain each activity in one sentence.



Part 3 – Challenge Questions

1. What is the difference between traditional risk management and more current risk management approaches?

2. What is the difference between penetration testing and red teaming

3. One of the main goals in the Cyber Threat Intelligence process is to extract intelligence from information. What is the purpose of doing that and what are 3 differences between information and intelligence?

4. If you had limited budget available, which of the NIST IR process phases (Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-Incident activity) would you focus your resources on and explain why?

5. If you are in the management team in an organization, which skills should you possess to be able to handle crisis situations effectively? Why?