EXAM CYBER SECURITY MANAGEMENT - FEBRUARY 02, 2017

Course Code: 201500041/201500018 START TIME: 13.30H END TIME: 16.30H

GRADING: (NUMBER OF POINTS + 2)/10

Governance and Risk Management (10 points)

- 1. **(1 point)** Name four goals of information security governance and give a brief explanation of these goals. One sentence per goal is enough.
- 2. The three lines of defense model for risk management was covered in the additional literature used in Lecture 1.
 - a. (1 point) Give for each line of defense a brief description of both the core activity that is universal for all organizations as well as the motivation for having this line of defense in place.
 - b. **(0.5 points)** Which practices would you recommend to an organization to specify duties according to the three lines of defense model? Name two.
- 3. **(2 points)** Mentality towards cyber risk and management thereof has evolved a lot in recent years. Give a brief description of three important trends in cyber risk management.
- 4. **(2 points)** Four roles in information security governance have been discussed in Lecture 1. Complete the table below by filling in the gaps, and by reordering and matching the roles from the left-hand column with the responsibilities in the right-hand column.

Roles	Responsibilities
Board of directors / senior	
management	
Executive management	
	Accountability, high-level understanding of risk, endorsement, alignment with the business strategy
	Creation and effectiveness of information security program, establishing communication channels and obtaining senior management commitment

- 5. Quantification of cyber risk was treated in Lecture 1.
 - a. **(1 point)** Indicate how quantifying cyber risk can lead to knowing the return on investment of security projects.
 - b. (1 point) Name two challenges that an implementation of cyber risk quantification in organizations has to overcome in order to be successful.
- 6. (3 x 0.5 points) Mark whether the statements below are true or false and briefly explain why this is so.
- Because information security is the responsibility of everyone in the organization, it is crucial that everyone in the organization attends the same security awareness course.
- Organizations should use a framework when defining and realizing information security governance.
- Using annual loss expectancy as a quantity on which risk management is based avoids a false sense of security.

SUS At your own Mar of wourt relief

CONTRACTOR 20150001/20150018

Of \((S + ETMEN OF SHEWN H) DEPENDED

Governance and Risk Management (10 points)

- (1 paint) stand four goals of information security governance and give a lister explination of this secure. One sentence per goal is enough.
 - Tiet these lines of defense model for risk management was concern in the additional
 - a. (1 point) Give for each line of defense a brief description of both the core activity that is universal for all organizations as well as the motivation for having this line of defends or december.
 - 0.5 points) Which practices would you recommend to an organization to specify deber-
- (2 points) identality towards cyber risk and management thereof her evolved a lot in recent units, over a confidenciation of three important trends in cyber risk entragement.
 - (2 points) For a roles in intermation security governance have been discussed in Lecture 1.
 Complete the table below by tilling in the gaps, and by representing and matching the roles.
 Thus, the left hand column with the responsibilities in the right hand column.

- quantification of cyber risk was treated in Lecture 1.
- (1 point) indicate how quantifying cyber risk can lead to knowing the return on investment of security projects.
- (1 paint) Name two challenges that an implementation of cyber rist quantification in preparations has so overcome in order to be successful.
- (i. 3 x 9 5 points) Mark whother the statements below are true or faire and briefly explain why this is so
- Recause information security is the maponsibility of everyone in the organization, it is studied that everyone in the organization attends the same security aware ress course. Organizations should use a framework when defining and realizing information security.
- Using annual loss expectancy as a quantity on which risk management is based evoids a false sense of security.

Identity and Access Management (10 points)

- (2 points) Besides "something you know", like a password or PIN, there are additional methods you can authenticate with. Name the other two methods and provide 2 examples per method.
- 2. **(2.5 points)** Lecture 2 introduced the FIDO Alliance and used the FIDO overview of the U2F protocol as a reading material. Explain what the FIDO Alliance is, what their goal is, and what the difference is between the protocols UAF and U2F?
- 3. **(2 points)** Consider a situation in which access has been gained with a trust level that is not sufficient. What method can be applied to request additional authentication of the user in this case, considering the resource for which access is requested and the risk associated with that resource. Based on what information can this method operate?
- 4. **(2 points)** Identity & Access management consists of three key elements, identification, authentication and authorization. Explain each of these three elements in one sentence per element.
- 5. **(1.5 points)** There are four levels of authentication / identity proofing based on STORK and ISO29115: Low, Medium, High, Very High. Describe three differences between Medium and High.

Industrial Control Systems (8 points)

- 6. **(1.5 points)** Explain the elements and the working principle of a basic control loop in industrial control systems (ICS). Provide an example of an industrial process and explain how basic control loop is implemented in it.
- 7. **(1.5 points)** Bailey and Wright describe notion of 5 levels of hierarchy in ICS architecture concept. Enumerate all levels and briefly explain their role.
- 8. (0.5 points) What are two advantages and two disadvantages of using data diode in ICS?
- 9. (3 x 0.5 points) ICS environments highly depend on human operators.
 - A. Name key elements required for **user** operation in ICS;
 - B. Name two scenarios how a human interface be (un)intentionally misused to cause a cyber incident in ICS?
 - C. What are available data sources for monitoring user activity for potential cyber threats?
- 10. **(4 x 0.5 points)** IT and ICS environments differ in multiple design and implementation characteristics. These characteristic have implications on application of security controls in ICS. Please provide short answers (1 sentence) to the following questions:
 - A. How are CIA (Confidentiality, Integrity, Availability) principles of information security prioritized in IT vs ICS?
 - B. What is component lifetime in IT vs ICS?
 - C. What are the key differences between IT and ICS with respect to architecture and network protocols?
 - D. How is change management implemented in IT vs ICS?
- 11. (4 x 0.25 points) Mark all correct statements:
 - A. It is not possible to perform a MitM attack on an ICS network since PLCs talk proprietary protocols.
 - B. There is a low requirement for time-critical interaction between components in ICS systems.
 - C. An attacker can discover functional implementation of Modbus TCP protocol by interacting with a PLC which uses that protocol.
 - D. Signature-based IDS perform with following characteristics: 0% false positive and 0% false negative.

Identity and Access Management (19 points)

- (2-paints) bendes "something you know", like a payayord or Prit, there are address in netheral you are authenticate with Name the other two methods and provide 3 coungles are method.
- (2.5 points) critime 2 retroduced the F100 Aliance and cred the HDD eventiew of the U2F personal is a resoling material. Explain what the F100 Aliance is what their goal is and what the difference is between the correction UAF and U2F?
- (3 points) Consider a situation in which access has been gamed with a Lost texel that is not sufficient. What method can be applied to request additional authorization of the care as this case, considering the essence for which access is requested and the risk associated with the reserver. Butted on what information can this certical access section.
- (2 paints) identified Access management consists of three key elements, identificance authorized on and authorized on Explain each of these three elements in one sentence necleoners.
- (3.5 points) There are four levels of authentication / identity proofing based on STORS and is 229115 tow. Medium, Tigh Very High Describe three differences in pasen Medium and relations.

dustrial Control Systems (8 points)

- (1.5 paints) i sature the elements and the working principle of a basic control loop in industrial correct systems (ICS). Provide an example of an industrial process and examin how basic control loop is implemented in it.
 - (3.5 points) saley and Whatt describe notion of 5 levels of hierarchy in ICS architecture concept. Enumerate all levels and briefly explain their role.
 - (d.5 points) What are two udvantages and two disadvantages of using data diode.
 - c. (3 x 0.5 points) ICS environments highly depend on human operators
 - Marine key elements required for user operation in ICS;
- By Many two scenarios haw a human interface by (un)intentionally mixtured to course a cubor incident in ICE?
 - where are available data sources for monitoring user activity for potential cytics (areats?)
- (4 x 0.5 points) If and ICS environments differ in multiple design and implementation
 Characteristics, These sharecteristic have implications on application or security controls in
 - Please provide short answers () septence) to the following questions:
- How are CIA (Confidentiality, Integrity, Availability) principles of ellochastics security
 procritized in IT vs ICS?
 - LOW BY BE IN SANDOWN TO BE ON THE PER SECTION OF TH
 - C. What are the key differences between IT and ICS with respect to architecture and
 - D. How is change management implemented in IT vs ICS?
 - t sign and a state of the state
 - A It is not possible to perform a MitM attack on an ICS network since PECs (all
- There is a low requirement for time-critical interaction between components in ICS
 - en attacker can discover functional implementation of Modbus TCP protocol by
- Signature-based IDS perform with following characteristics ON false positive and ON false negative

Physical and Social Security (10 points)

- 12. (2 points) When is the right time to do Open Source Intelligence and overall reconnaissance?
- 13. **(2 points)** Which are the different types of reconnaissance? Provide an example activity for each type.
- 14. **(2 points)** Name common protection mechanisms for Human, Cyber and Physical security and rate effectiveness in terms of social engineering.
- 15. **(2 points)** What is the difference between penetration testing and red teaming, and explain how penetration testing and red teaming differ.
- 16. **(2 points)** Explain the human condition and the "Parent, Adult, Child" relationship. How does this apply into Social Engineering?

Security Monitoring (10 points)

- 17. A. (1 point) What is the difference between a NIDS and a HIDS? Name at least two differences.
 - B. (2 points) Explain two advantages of NIDS over HIDS and vice versa.
 - C. (1 point) Which type of attack would a NIDS detect, but not a HIDS?
- 18. Building a World-Class Security Operations Center: A Roadmap (SANS, 2015) describes different techniques for security monitoring.
 - A. (1.5 points) In the context of security monitoring: Explain the difference between baselining and correlation, and name at least 2 advantages of baselining over correlation.
 - B. **(1.5 points)** Name 4 processes that go on in a Security Operations Center. Which two are the most important, and why?
- 19. **(1 points)** The ISACA paper (as well as Lecture 5) presents Security Information & Events Management (SIEM). What are two examples of business context data to use in a SIEM?
- 20. Big Data Analytics for Security (Cárdenas, 2013) explains the capabilities of data analytics for security purposes
 - A. (1 point) Explain why 'traditional' security technologies are not able to support analytics capabilities.
 - B. **(1 point)** Describe how data analytics tools are able detect advanced persistent threats (APTs).

Managed Security Services (MSS) (10 points)

- 21. **(1 point)** Which factors drive the cost of offering an MSS (as in, the costs incurred by an MSS provider) and explain why? Name three.
- 22. **(1 point)** Which factors play a role in the pricing of an MSS (as in, the price charged by an MSS provider) and explain why? Name three.
- 23. **(1 point)** Explain 2 reasons for an organization to want to keep a function in-house, and 2 for contracting a service provider to do it.
- 24. **(0.25 points)** Name an example of an information security function that is commonly provided by MSS providers.
- 25. **(1.5 points)** How do the types of services contracted from MSS providers relate to an organization's security maturity?
- 26. (0.75 points) Name three important criteria for selection of an MSS provider.
- 27. (1.5 points) Why are not all MSS providers included in analyses by market analysts?
- 28. **(2 points)** Which types of MSS providers can you distinguish? Name four types of organizations, and indicate their market approach.
- 29. Cloud Access Security Brokers (CASB) were discussed during the lecture.

Physical and Social Security (10 points)

- (2 juints) When it the right time to do Open Source Intelligence and exceed reconcursance?
 - points) who is are the different types of reconnaissance. Provide as us emple adjusts for each tree.
 - (2 points) his ne common proceetion mechanisms for Human, Cabra and Physical recurity and rate effectiveness in terms of social engineering.
 - (2 points) What is the difference between penetration resurg and and reading and explain.
 I my genetration resting and real reaming differ.
- (2 points) Envision (for human condition and the "Parent, Adult, "field" cristionship. Here does (int. apply into Social Engineering?

Security Monitoring (30 points)

- The A. (1 point) What is the difference between a MDS and a MDS? Name of least two differences
 - I replace) Explain two advantages of MIDS over MIDS and vice until
 - C. L. patinti, Which type of attack would a MIDS detect, but not a MIDS."
- defending a World-Class Security Operations Center: A Roadman (SANS, 2015) describes
- (1.5 points) in the context of security monitoring. Explain the difference between caseform and correlation, and name at least 2 advantages of baseloning over correlation
- (1.8 points) Name 4 processes that go on in a Security Operation. Center. Which two are the most emperiority and why?
 - [4] [1 polints] The ISACA paper (as well as Lecture 5) presents Security Information & Events (significant (SIEM)). What are two examples of business context data to use in a SIEM?
- 20 Sty Data Analytics for Security (Cardenas, 2013) explains the capabilities of data analytics for security purposes.
- (I point) Expisin why traditional security rechnologies are not able to support analytics readilities.
- [1 point] Describe how data analytics tools are able detect advanced persistent threats

Managed Security Services (MSS) (10 points)

- (1 point) Which factors drive the cost of offering an MSS (as in, the casts incurred by an WSS provider) and explain why? Name three:
 - 22 (1 point) Which factors play a role in the pricing of an MSS (as in the price charged by an MSS provider) and explain why? Mante three.
- 23 (I point) Explain 2 reasons for an organization to want to keep a function in-house, and 2 for contracting a service provider to do it.
 - 24. (6.25 points) Name an example of an information security function that is commonly drovided by MSS providers.
 - (L.S points) How do the types of services contracted from MSS providers relate to an depolitation's security maturity?
 - a the vs agints) Marrie three important criteria for selection of an MSS provider.
 - 27. ILS points) Why are not all MSS providers included in analyses by market analysis.
 - 28. (a points) Which types of MSS providers can you distinguish? Name four types of presentations, and indicate their market approach.
 - tend access security tendens (CASB) were discussed during the lecture

- A. **(0.5 points)** What is the distinguishing feature of a CASB, compared to a non-CASB MSSP?
- B. (0.5 points) Which types of services are typically offered by CASBs?

Incident Response (10 points)

- 30. **(3 points)** Name the different **phases** in the incident response life cycle according to the NIST Security Incident Handling Guide (the reading material in Lecture 7). For each phase, provide 3 examples of activities you perform within that phase.
- 31. **(2 points)** Consider a situation in which your organization has received signals of a possible data breach. Your IT administrators only have outdated network designs. Describe which key actions you would take. Motivate your answer.
- 32. (2 points) Describe 2 things you would consider when gathering and analyzing volatile data?
- 33. **(1 point)** According to the NIST Security Incident Handling Guide, what are the three possible team models for incident response teams?
- 34. **(1 point)** Which activity is the most important to perform after an incident has been resolved (but is often overlooked)?
- 35. **(1 point)** Your system administrator notices one of the servers is missing log files of one specific day. Would you start the incident response process? Motivate your answer.

Crisis Management and Business Continuity (10 points)

- 36. **(1 point)** What is the difference between an incident and a crisis? In your answer, use the three key elements that Boin et.al. **(2005)** use to define a crisis.
- 37. **(1 point)** Explain what group think is, and how it can affect the decision making process during crises.
- 38. **(3 points)** Successful organizations are capable to *prepare* in advance for unforeseen (potentially) disruptive events, *respond* effectively to crisis situations and *recover* from them successfully.
 - a. **(0.75 points)** Name and describe the building blocks that organizations should have in place preparing for crises.
 - b. **(0.75 points)** In the lecture, we mentioned a decision making process that crisis management teams should apply when responding to and managing crises. Describe the steps of this process.
 - c. **(0.75 points)** Explain why evaluations are an important part of the recovery phase of crises.
 - d. **(0.75 points)** How would the approach (preparation, response, recovery) for dealing with a cyber crisis be different from the approach for dealing with other crisis types?
- 39. **(2.5 points)** In the paper 'The Politics of Crisis Management', Boin et.al. **(2005)** define five critical tasks in crisis leadership.
 - a. Name these five tasks and provide a description per task.
 - b. For each task, describe at least one challenge that crisis leaders are confronted with in executing these tasks.
- 40. **(2.5 points)** Communication to internal and external stakeholders is an important part of crisis management.
 - a. (0.5 points) Explain why communication is a critical function in crisis management.
 - b. (1.25 points) Seegers (2006) describes ten best practices of crisis communication.
 Name five of these best practices, and explain why they are important.
 - c. (0.75 points) How did social media change the crisis management landscape?

(9.5 points) What is the distinguishing feature of a CASB, compared to a non-CASB MSSE?

titls enional Whith Issues of someoes are (version of orest bor ASBS)

incident Response (18 paints)

(3 points) Nume the different phases in the incident in soonse of cycle according to the MST sounty incident Harding Guide (the reading material in Lecture 7) for each phase, provide a sounder of activities you perform within that phase

(3 goints) Consider a situation in which your organization has received agrain ut a possible data breach. Your IT administrators only have outdated network design: Treatible which ket allians you would take. Notivate your answer.

22. (a points) Describe Zithings you would consider when gathering and analyzing volume detect

33. (1 point) According to the NIST Security Incident Handling Guide, what are the times possible than models for incident response seams?

cat. (a coint) Which activity is the most important to perform after an incorne has be un

(1 point) Your system administrator notices one of the servers is massing log files of one specific day. Would your start the incident response process? Motivate your answer.

rigis Management and Susiness Continuity (10 points)

(i) policy) what is the difference between an incident and a costs? In your answer, use the three key starpents that Boin et al. (2005) use to define a cross.

37 (1 point) isolain what group think is, and how it can affect the decision making process during crises.

8 (a points) Successful organizations are capable to prepare in advance for unforeseen (noternially) disruptive events, respond offectively to crisis situations and recover from them duccessfully.

(9.75 points) Name and describe the building blocks that organizations should have a preparing for crises.

b. (8.75 paints) in the locture, we membaned a decision making process that crisis management teams should apply when responding to and managing crises. Describe the state of this process.

(c. 75 paints) Explain why evaluations are an important part of the recevery phase of enses.

d (0.75 paints) How would the approach (preparation, response, recovery) for dealing with a cyber cross be different from the approach for dealing with other cross types?

2.5 points) in the paper 'The Politics of Crisis Management', Soin et al. (2003) Define Tive

Marine Bresse five tasks and provide a description per task

 b. For each task, describe at least one challenge that crisis leaders are confronted with in executing these tasks.

40. (2.5 coints) Communication to internal and external stakeholders is an important part of

a (0.5 milits) Explain why communication is a critical function in crisis management

(1.25 points) Suegers (2006) describes ten best practices of crisis communication. Manne five of these bast practices, and explain why they are important.

(0.75 points) How did social media change the crisis management landscape?