M10A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 10 of textbook

DATE ASSIGNED: April 7, 2020 DATE DUE: April 13, 2020 POINTS: 25

[A, 6 points] Multiple Choice

[A1] Prior to 1980, the responsibility for computer security rested with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.(c)

(a) users (b) programmers (c) computing center staff

[A2] Today, a significant amount of responsibility for computer security has shifted to

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) users (b) programmers (c) computing center staff

[A3] \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ forms the basis for describing the current status of security. (a)

(a) Risk Analysis (b) Business Continuity

[A4] Besides the Security Plan, a Business \_\_\_\_\_\_\_\_\_\_\_\_\_ Plan is recommended for companies. (a)

(a) Continuity (b) Response

[A5] Besides the Security Plan, an Incident \_\_\_\_\_\_\_\_\_\_\_\_ Plan is recommended for companies. (b)

(a) Continuity (b) Response

[A6] \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a US government program under which computer equipment is

certified as emission-free. (a)

(a) Tempest (b) Storm

[B, 19 points] For each of the following, state if it is TRUE or FALSE.

[B1] Every organization that uses computers to create and store valuable assets needs a security plan. (T)

[B2] Security requirements explain how security should be implemented. (F)

[B3] 80 percent of organizations affected by a significant computer incident close within 18 months. (F)

[B4] Natural disasters: floods, fire, storms, earthquakes, volcanic eruptions, etc. can neither be predicted nor prevented; but one must prepare for them. (T)

[B5] A magnetic disk can be “cleaned” , permitting it to be reused by others, by “overwriting” or by degaussing. (T)

[B6] Deciding whether , when, and how to back-up data is an essential business decision. (T)

[B7] The backup must not also be destroyed in the disaster, so offsite backups are recommended. (T)

[B8] Offsite backups can be provided by Networked Storage and by Cloud Backups. (T)

[B9] When producing the Security Plan, the Security Planning Process takes the following inputs:

Requirements, Constraints, Mechanisms. (T)

[B10] A Business Continuity Plan need not deal with *catastrophic situations* in which all or part of

computing capability is unavailable. (F)

[B11] A Business Continuity Plan need not deal with *long duration* situations in which the outage is

expected to last for so long that business will suffer. (F)

[B12] An Incident Response Plan should not define what constitutes an incident. (F)

[B13] An Incident Response Plan should identify who is responsible for taking charge

of the situation. (T)

[B14] Risk Impact x Risk Exposure = Risk Probabilty. (F)

[B15] Cost of reduction =

(Risk exposure before reduction - Risk exposure after reduction )/ Risk Leverage

(T)

[B16] Three strategies for dealing with risk are: avoid risk, transfer risk, assume risk. (T)

[B17] Three approaches to preventing theft are: preventing access, preventing portability,

detecting exit. (T)

[B18] Power supply problems cannot be alleviated using Uninterruptible Power Supplies and Surge

Suppressors. (F).

[B19] Emanations from a device cannot be prevented by shielding the device completely in a

copper case. (F)