Module 4: True or False questions

1. [✓ T]/F One of the ways in which business and cybersecurity overlap is that businesses must ensure their computer systems and networks are secure.
2. [✓ T]/F One of the ways in which business and cybersecurity overlap is that cybersecurity businesses have been created.
3. [✓ T]/F One of the ways in which business and cybersecurity overlap is that businesses may either commit cybercrimes or be victims of cybercrime.
4. [✓ T]/F One of the ways in which business and cybersecurity overlap is that all employees have a role in protecting business computer systems and networks.
5. [✓ T]/F Businesses must ensure systems are secure due to business goals.
6. [✓ T]/F Businesses must ensure systems are secure due to legal reasons.
7. [✓ T]/F Businesses must ensure systems are secure due to financial motivations.
8. [✓ T]/F Businesses must ensure systems are secure due to employee morale.
9. T/[✓ F] Businesses must ensure systems are secure due to business goals but not to legal reasons.
10. T/[✓ F] Businesses must ensure systems are secure due to legal reasons but not financial ones.
11. T/[✓ F] Businesses must ensure systems are secure due to financial motivations but not employee morale.
12. [✓ T]/F Strong information security in businesses is a sign of good management.
13. [✓ T]/F Strong information security in businesses is a sign of good customer service.
14. [✓ T]/F Strong information security in businesses is a sign of good economic thinking.
15. T/[✓ F] Strong information security in businesses is a sign of good bureaucratic control.
16. T/[✓ F] Strong information security in businesses is not a sign of good management.
17. T/[✓ F] Strong information security in businesses is not a sign of good customer service.
18. T/[✓ F] Strong information security in businesses is not a sign of good economic thinking.
19. [✓ T]/F Business goals should protect confidentiality, integrity and availability of information.
20. T/[✓ F] Failing to protect civil liberties of consumers is not placing businesses at risk.
21. T/[✓ F] Failure to protect data may result in bad reviews for companies but not liability for lawsuits.
22. T/[✓ F] Companies do not have an obligation to notify authorities when breach occurs.
23. [✓ T]/F Companies have an obligation to notify authorities when breach occurs.
24. [✓ T]/F Businesses may suffer internal and external losses as a result of insufficient information security.
25. T/[✓ F] Businesses may suffer internal but not external losses as a result of insufficient information security.
26. T/[✓ F] According to Ponemon’s study, the country with highest average losses is Russia and with the lowest – India.
27. T/[✓ F] According to Ponemon’s study, the country with highest average losses is China and with the lowest – Russia.
28. T/[✓ F] According to Ponemon’s study, the country with highest average losses is the U.S. and with the lowest – Saudi Arabia.
29. [✓ T]/F According to Ponemon’s study, the country with highest average losses is the U.S. and with the lowest – Russia.
30. [✓ T]/F Businesses in the health care sector have ethical duty to protect information.

31. [✓ T]/F Businesses in the law sector have ethical duty to protect information.
32. [✓ T]/F Businesses in the education sector have ethical duty to protect information.
33. T/[✓ F] Businesses in the health care sector do not have ethical duty to protect information.
34. T/[✓ F] Businesses in the law sector do not have ethical duty to protect information.
35. T/[✓ F] Businesses in the education sector do not have ethical duty to protect information.
36. T/[✓ F] Cyber operation businesses include functions as reverse engineering but not software development.
37. T/[✓ F] Cyber operation businesses include functions as crisis management but not malware analysis.
38. T/[✓ F] Cyber operation businesses include functions as network engineering but not on-demand cybersecurity.
39. [✓ T]/F Cyber operation businesses include functions as network engineering, on-demand cybersecurity and software development.
40. T/[✓ F] Products or services related to cybersecurity that companies sell include anti-virus software, security platforms, data analytics, administrative policy recommendations, and data protection.
41. [✓ T]/F Products or services related to cybersecurity that companies sell include anti-virus software, security platforms, data analytics, and data protection.
42. T/[✓ F] Cyber incidents are typically covered by traditional corporate insurance policies.
43. T/[✓ F] Cyber incidents are not typically covered by traditional insurance policies.
44. T/[✓ F] Cyber liability coverage could cover liability for breaches but not expenses from cyber extortion and terrorism.
45. T/[✓ F] Cyber liability coverage could cover liability for breaches but not expenses from cyber extortion and terrorism.
46. [✓ T]/F Cyber liability coverage could cover liability for breaches, cyber extortion and terrorism and costs for restoring businesses.
47. T/[✓ F] One of the biggest similarities between white-collar crime and cybercrime is that they both have an international focus.
48. T/[✓ F] One of the biggest similarities between white-collar crime and cybercrime is that they both include older offenders.
49. T/[✓ F] One of the biggest similarities between white-collar crime and cybercrime is that none of them is seen as a national threat.
50. T/[✓ F] One of the biggest differences between white-collar crime and cybercrime is that the former has specialized police units designed to respond to them but the latter does not.
51. [✓ T]/F One of the biggest similarities between white-collar crime and cybercrime is that neither are central to the study of crime and criminal justice.
52. [✓ T]/F Contrepreneurial white-collar cybercrime is cybercrimes committed in course of illegitimate enterprise.
53. T/[✓ F] Contrepreneurial white-collar cybercrime is cybercrimes committed in course of legitimate enterprise.
54. [✓ T]/F Changes in consumer behaviors lead to changes in crimes are related to the trends in white-collar cybercrime.
55. T/[✓ F] Females typically commit white-collar cybercrime alone more often than as accomplices.