New Zealand Cyber Security Challenge 2018
Round Two Answers

1. A standard is
   a) A document that sets out the minimum specifications that a product, process or service needs to comply with, before it can be used in a production environment. This may include characteristics such as security aspects or performance requirements.
   b) A high level statement of an organisation’s vision in cyber security.
   c) A methodology for a prescriptive, step-by-step set of activities based on best practices, models and guidelines.
   d) A legally binding requirement made by bodies of industry and government departments that that individuals and organisation’s need to comply with in order to avoid penalties/prosecution.

2. While working on the 2018 Cyber Security Challenge, Bob a security analyst, has found a flaw in the underlying platform to allow an unauthenticated user access to execute arbitrary code and access the database table containing username and passwords. He wants to be responsible and disclose the flaw. When reporting the security flaw to CROW, which of the following information violates the expectations of a responsible disclosure?
   a) A press release about the flaw to the media without prior approval and consultation with CROW.
   b) A press release about the flaw to the media with prior approval and consultation with CROW.
   c) A proof of concept about the flaw demonstrating the exploitation and likely impact.
   d) An email containing the list of the revealed usernames and passwords sent to CROW to inform its staff.

3. A defence contracting company would like to add an administrative security control that protects against insider attacks. Which one of the following controls best meets those criteria?
   a) Background checks
   b) Data loss preventions system
   c) Penetration tests
   d) Vulnerability scans

4. You are given the following statement:
   “A process to follow when implementing a change to the network or system”
   What is the name of the policy is this describing?
   a) Change management policy
   b) Change execution policy
   c) Risk mitigation policy
   d) Risk implementation policy

5. You are given the following statement:
“Used to educate employees and customers as to how and why information is collected from Its customers and how that information will be used”
What is the name of policy is this describing?
   a) Data collection policy
   b) Data privacy policy
   c) Information usage policy
   d) Information security policy

6. What is an example of an occurrence for which the business continuity plan (BCP) would be activated?
   a) An employee is disgruntled and threatening to keep his company issued mobile phone if he is terminated.
   b) A supervisor notices that an employee is using a company issued device to access their personal email, even after being instructed not to.
   c) A flood from a natural disaster has occurred in the building in which the organization's servers are kept and they are under water.
   d) A manager has noticed that her employee has been late five days in a row and is falling behind in work.

7. While at work Alice decides to look for a new house and cheap air tickets during work hours. Which Policy has she likely breached by doing this?
   a) Working hours policy
   b) Internet usage policy
   c) Integrity policy
   d) Company travel policy

8. What is the most critical factor in the development of a disaster recovery plan (DRP) of a critical infrastructure provider?
   a) Business impact analysis (BIA)
   b) Contact numbers of every staff member
   c) Participation from every department
   d) Management support

9. The development of an IS security policy is ultimately the responsibility of the:
   a) Information security department.
   b) Security committee.
   c) Security administrator.
   d) Board of directors

10. What is the title of the NZ legislation will lay out offenses/crimes which involve the use of computers?
    a) Crimes Act 1961
    b) Government Communications Security Bureau Act 2003
    c) Telecommunications (Interception Capability and Security) Act 2013
    d) Computer Legislation Act 2010

11. The PRIMARY objective of an audit of a company's IT security policies is to ensure that:
    a) they are distributed and available to all staff.
    b) security and control policies support business and IT objectives.
    c) there is a published organizational chart with functional descriptions.
    d) duties are appropriately segregated.

12. A teacher of a high school was fired after a serious criminal offence reported by the principal. The teacher deleted all student databases before he left the job and school campus. This happened just before the examinations period and the school is heavily impacted. What could have been the BEST way to prevent this from happening?
    a) Creation of an information security management system (ISMS) for the school.
    b) Preventing USB stick access for all computers.
    c) Card access for all teaching and server rooms.
    d) Creation of a data privacy policy and staff integrity policy.

13. You are the security expert in Company A, and its staff have recently been subject to phone-based social engineering attacks. From a business point of view, how would you BEST reduce the risks of important information leaked out by staff answering potential social engineering phone calls?
    a) Creating and implementing scripts for staff to use when they take phone calls.
    b) Send a fake employee to trick staff regularly with social engineering attacks to increase resiliency of the company.
    c) Remove phones for staff who do not make phone calls regularly.
    d) Patching your staff desktops every half a day.

14. Alice is a student at the University of Waikato, as part of one of her computer science papers she needs to conduct a survey. She tells the participants the purpose of the survey and what she will be doing with the data. After she has collated it all, her friend asks her if she can use the names to sign them up to the University Sports Club Newsletter. Which number privacy principle of the Privacy Act will be breached if she does this?
    a) Principle 3: Collection of information
    b) Principle 8: Accuracy of personal information to be checked before use
    c) Principle 6: Access to personal information
    d) Principle 10: Limits on use of personal information

15. Which of the following is NOT a countermeasure to traffic analysis?
    a) Padding messages.
    b) Eavesdropping.
    c) Sending noise.
    d) Using a Faraday Cage