Correct Answer: D
Explanation:
To be effective a patch management program must be in place (due diligence) and detailed procedures would specify how and when the patches are applied properly (Due Care). Remember, the question asked for NOT a violation of Due Diligence, in this case, applying patches demonstrates due care and the patch management process in place demonstrates due diligence.

Due diligence is the act of investigating and understanding the risks the company faces. A company practices by developing and implementing security policies, procedures, and standards. Detecting risks would be based on standards such as ISO 2700, Best Practices, and other published standards such as NIST standards for example.

Due Diligence is understanding the current threats and risks. Due diligence is practiced by activities that make sure that the protection mechanisms are continually maintained and operational where risks are constantly being evaluated and reviewed. The security policy being outdated would be an example of violating the due diligence concept.

Due Care is implementing countermeasures to provide protection from those threats. Due care is when the necessary steps to help protect the company and its resources from possible risks that have been identifed. If the information owner does not lay out the foundation of data protection (doing something about it) and ensure that the directives are being enforced (actually being done and kept at an acceptable level), this would violate the due care concept.

If a company does not practice due care and due diligence pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence. Liability is usually established based on Due Diligence and Due Care or the lack of either.

A good way to remember this is using the first letter of both words within Due Diligence (DD) and Due Care (DC).

Due Diligence = Due Detect
Steps you take to identify risks based on best practices and standards.

Due Care = Due Correct.
Action you take to bring the risk level down to an acceptable level and maintaining that level over time.

The Following answer were wrong:

Security policy being outdated:
While having and enforcing a security policy is the right thing to do (due care), if it is outdated, you are not doing it the right way (due diligence). This questions violates due diligence and not due care.

Data owners not laying out the foundation for data protection:
Data owners are not recognizing the "right thing" to do. They don't have a security policy.

Network administrator not taking mandatory two week vacation:
The two week vacation is the "right thing" to do, but not taking the vacation violates due diligence (not doing the right thing the right way)

Reference(s) used for this question:
Shon Harris, CISSP All In One, Version 5, Chapter 3, pg 110

QUESTION 471
A host-based IDS is resident on which of the following?

A. On each of the critical hosts
B. decentralized hosts
C. central hosts
D. bastion hosts

Correct Answer: A
Explanation:
A host-based IDS is resident on a host and reviews the system and event logs in order to detect an attack on the host and to determine if the attack was successful. All critical serves should have a Host Based Intrusion Detection System (HIDS) installed. As you are well aware, network based IDS cannot make sense or detect pattern of attacks within encrypted traffic. A HIDS might be able to detect such attack after the traffic has been decrypted on the host. This is why critical servers should have both NIDS and HIDS.

FROM WIKIPEDIA:
A HIDS will monitor all or part of the dynamic behavior and of the state of a computer system. Much as a NIDS will dynamically inspect network packets, a HIDS might detect which program accesses what resources and assure that (say) a word-processor hasn\'t suddenly and inexplicably started modifying the system password-database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file- system, or elsewhere; and check that the contents of these appear as expected.

One can think of a HIDS as an agent that monitors whether anything/anyone - internal or external - has circumvented the security policy that the operating system tries to enforce.
http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

QUESTION 472
Which of the following is most likely to be useful in detecting intrusions?

A. Access control lists
B. Security labels
C. Audit trails
D. Information security policies

Correct Answer: C
Explanation:
If audit trails have been properly defined and implemented, they will record information that can assist in detecting intrusions.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 186).

QUESTION 473
Which of the following tools is NOT likely to be used by a hacker?

A. Nessus
B. Saint
C. Tripwire

D. Nmap

Correct Answer: C
Explanation:
It is a data integrity assurance software aimed at detecting and reporting accidental or malicious changes to data.

The following answers are incorrect:

Nessus is incorrect as it is a vulnerability scanner used by hackers in discovering vulnerabilities in a system.
Saint is also incorrect as it is also a network vulnerability scanner likely to be used by hackers.
Nmap is also incorrect as it is a port scanner for network exploration and likely to be used by hackers.

Reference :
Tripwire : http://www.tripwire.com
Nessus : http://www.nessus.org
Saint : http://www.saintcorporation.com/saint
Nmap : http://insecure.org/nmap

QUESTION 474
How often should a Business Continuity Plan be reviewed?

A. At least once a month
B. At least every six months
C. At least once a year
D. At least Quarterly

Correct Answer: C
Explanation:
As stated in SP 800-34 Rev. 1:
To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.

Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within you exam.

Reference(s) used for this question:
NIST SP 800-34 Revision 1

QUESTION 475
In order to enable users to perform tasks and duties without having to go through extra steps it is important that the security controls and mechanisms that are in place have a degree of?

A. Complexity
B. Non-transparency
C. Transparency
D. Simplicity

Correct Answer: C
Explanation:
The security controls and mechanisms that are in place must have a degree of transparency.

This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.

Security (more specifically, the implementation of most security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users, forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user.

For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area.

In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent. A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference.

When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as little as possible.

The following answers were incorrect:
All of the other detractors were incorrect.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th edition. Operations Security, Page 1239-1240
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25278-25281). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Access Control ((ISC)2 Press) (Kindle Locations 713-729). Auerbach Publications. Kindle Edition.

QUESTION 476
Attributable data should be:

A. always traced to individuals responsible for observing and recording the data
B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data

Correct Answer: A
Explanation:
As per FDA data should be attributable, original, accurate, contemporaneous and legible. In an automated system attributability could be achieved by a computer system designed to identify individuals responsible for any input.
Source: U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry - Computerized Systems Used in Clinical Trials, April 1999, page 1.

QUESTION 477
Why would anomaly detection IDSs often generate a large number of false positives?

A. Because they can only identify correctly attacks they already know about.
B. Because they are application-based are more subject to attacks.
C. Because they can't identify abnormal behavior.
D. Because normal patterns of user and system behavior can vary wildly.

Correct Answer: D
Explanation:
Unfortunately, anomaly detectors and the Intrusion Detection Systems (IDS) based on them often produce a large number of false alarms, as normal patterns of user and system behavior can vary wildly. Being only able to identify correctly attacks they already know about is a characteristic of misuse detection (signature-based) IDSs. Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. They are more vulnerable to attacks than host- based IDSs. Not being able to identify abnormal behavior would not cause false positives, since they are not identified.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 92).

QUESTION 478
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files
D. Displayed the contents of a folder

Correct Answer: D
Explanation:
Displaying the directory contents of a folder can alter the last access time on each listed file.