**Course Name: Securing your network from Attacks**

*NOTE: Mark the correct answers with Yellow highlight*

**Chapter Number 3**

1. An insider threat…

a. Is a full time employee who hacks our network.

Incorrect, an insider threat can be an employee, contractor, ex-employee, or someone who has inside knowledge of our network and/or organization.

b. Is a virus that attacks our network from the inside.

Incorrect, an insider threat can be an employee, contractor, ex-employee, or someone who has inside knowledge of our network and/or organization.

c. Is a person on the inside who may or may not know they are taking action against our organization or network.

Correct, not all insider attacks are knowing participants. For example an employee this is social engineer to click a bad link can be a insider.

d. Is a type of phishing email

Incorrect, while a phishing email can lead to an insider attack, the email itself is not considers an insider attack.

2. Employee trainings….

a. Can be a critical part of our security posture.

Correct, our users tend to be primary targets for malicious hackers. Training our employees on identifying and reporting can be key to help protect them and our network.

b. Is not as critical as patching our computers and servers.

Incorrect, our users tend to be primary targets for malicious hackers. Training our employees on identifying and reporting can be key to help protect them and our network. While patching is good, a user can easily circumvent our security, knowingly and unknowingly.

c. Needs to be highly technical so our users know what the security team is dealing with.

Incorrect, having trainings that are overly complex will lose your users attention and understanding.

d. Are a waste of resources

Incorrect, our users tend to be primary targets for malicious hackers. Training our employees on identifying and reporting can be key to help protect them and our network.

3. When it comes to security and ease of use…

a. Security takes a front row every time.

Incorrect, locking down your network too much may result in users not being able to do their jobs effectively or at all.

b. A balance should be struck.

Correct, at the end of the day we need to both secure our network and allow our employees to operate efficiently.

c. Always make it easy, otherwise your employees will never comply

Incorrect, while we do need to make sure that our employees can do their day to day operations effectively, we also need to make sure our network is secure.

d. Employee’s will always be willing to follow strict security.

Incorrect, while there is a reasonable expectation that employees will follow security protocol, making it too strict may result in a backlash or inability to perform day to day operations effectively.

4. When it comes to employee reporting…

a. There needs to be total accountability for who reports an issue.

Incorrect, while some organizations may have this in place some employees may not report an issue due to embarrassment or fear of retribution.

b. Having the ability to report anonymously may be useful.

Correct, having a ability to report an issue anonymously can help those who are embarrassed or scared of retribution to report issues.

c. Is never as reliable as a network reporting tool.

Incorrect, while reporting tools can give great insight into a network, having a reporting tool for your employees can give you a much deeper look into other areas and attack vectors.

d. Should be done by a stringent reporting process in order to verify authenticity and lower false positives.

Incorrect, having employees go through a laborious process will likely result in lower report rates.

5. Also when it comes to reporting….

a. Employee’s should be terminated or punished for being reported, even if they report themselves.

Incorrect, while this may vary depending on the situation, being reported for example an employee who reports that they clicked on a phishing email should not be punished for that. They should receive additional training. Terminating or punishing people for small mistakes will lead to people not reporting in the future.

b. FAQ’s should not be used, they often lead to confusion.

Incorrect, having a good FAQ can cut down on user confusion and reporting that your security team and/or ID team will have to deal with.

c. Never outsource, this is a huge security risk.

Incorrect, you may have to consider an outside vendor that can handle this depending on how many reports are coming in and how large your organization is.

d. an easy to use FAQ is important.

Correct, having a good FAQ can cut down on user confusion and reporting that your security team and/or ID team will have to deal with.