Your grade: 100%

Your latest: **100%** • Your highest: **100%** • To pass you need at least 80%. We keep your highest score.

Next item

1. Imagine a company has experienced a network security threat resulting in the loss of customer data. Which potential impact is most likely to occur in this scenario? 1 / 1 point

- ○ Increased customer trust
- ◉ Financial impacts
- ○ Streamlined regulatory compliance
- ○ Expansion of market share

Correct
Correct! In the scenario described, the most likely potential impact of a network security threat resulting in the loss of customer data is financial loss. The company may incur costs associated with addressing the breach, such as investigating the incident, implementing remediation measures, and potentially compensating affected customers. Additionally, the loss of customer trust due to the breach may lead to a decline in revenue.

2. Which strategy for mitigating security threats is focused on deploying network monitoring tools and a security incident response plan? 1 / 1 point

- ◉ Monitoring and incident response
- ○ Educating users
- ○ Implementing defense-in-depth
- ○ Identifying vulnerabilities

Correct
Correct! The monitoring and incident response strategy is focused on network monitoring, developing a well-defined security incident response plan and regular testing and simulation.

3. One of the best practices for access control of your Cisco router or switch would be to: 1 / 1 point

- ○ Change default passwords and use strong, unique passwords for administrative access.
- ○ Use private VLANs (PVLANs) to isolate sensitive servers or devices from potential threats within the same VLAN.
- ◉ Enable port security to limit the number of MAC addresses allowed on an interface and prevent unauthorized devices from connecting.
- ○ Configure syslog or SNMP traps to send logs to a central server for analysis.

Correct
Correct! One best practice for access control of your Cisco router or switch is to enable port security to limit the number of MAC addresses allowed on an interface and prevent unauthorized devices from connecting. Access control is crucial for preventing unauthorized access and protecting sensitive information.