Knowledge Check Quiz Case Study Week 8 (JP Morgan)

Due Mar 13 at 11pm **Points** 13 **Questions** 13
Available until Mar 13 at 11pm **Time Limit** None

Instructions

Answer the following questions on the case study material this week.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	3 minutes	13 out of 13

Score for this quiz: **13** out of 13
Submitted Jan 27 at 3:27pm
This attempt took 3 minutes.

Question 1

1 / 1 pts

What was the **target of the attack**?

- Power Grid
- Bank

Correct!

- Water Services
- Energy Sector

Question 2

1 / 1 pts

Where did the attack occur?

Correct!

- [x] United States
- [ ] Ukraine
- [ ] Iran
- [ ] Australia

Question 3

1 / 1 pts

What was the **duration** of this attack?

Correct!

- [x] Months
- [ ] Hours
- [ ] Years
- [ ] Days

Question 4

1 / 1 pts

When was the attack **discovered**?

- [ ] December 2013
- [ ] March 2011

Correct!

- August 2014
- April 2007

Question 5

1 / 1 pts

What was the **impact** from the attack?

Correct!

- Customer records with contact information stolen
- Money stolen
- Widespread power outages
- Widespread ATM outages

Question 6

1 / 1 pts

What makes this case study **significant**?

- Supply chain attack to introduce counterfeit parts
- Insider attack on industrial control systems
- Denial of service attack as cyber warfare

Correct!

- Attack on company with significant cyber security budget and staff

Question 7

1 / 1 pts

How did the attack occur?

- Radio signals to SCADA devices causing pumps to fail
- Malware introduced in firmware updates
- Malware on employee's personal computer used to gain credentials

Correct!

- Distributed denial of service attack on government websites

Question 8

1 / 1 pts

What **technical concerns** contributed to this incident?

- Malware infected system accessed network through VPN

Correct!

- SCADA system insecure
- PING flood and botnets
- Adobe Flash vulnerability used to inject malicious code

Question 9

1 / 1 pts

What **human behavior** contributed to this incident?

- Contractor USB sticks used to install malware
- Employee with malware on personal computer

Correct!

- Coordinated cyber attack as political protest

- Disgruntled employee sabotaged operations

Question 10

1 / 1 pts

What **business decisions** contributed to this incident?

Correct!

- (selected) Two-factor authentication disabled on internal servers
- Old versions of Office and Windows
- Subcontractor with weak security practices given access
- Heavy dependence on IT services

Question 11

1 / 1 pts

Which technique to minimize the attack surface **prevents software from functioning unless it is on the approval list**?

- Antivirus and Regular Patching
- Employee Education

Correct!

- (selected) Application Whitelisting
- Intrusion Prevention System

Question 12

1 / 1 pts

Which techniques for protected enclaves **prevents a system from accessing a trusted network before it is scanned and checked**?

- Segregate Internal Network

Correct!

- (selected) Network Access Control
- Proxy with Outbound Traffic
- Protect Critical Assets

Question 13

1 / 1 pts

Which technique for monitoring, logging, and scanning is **attempting to gain access to a network without knowledge of the network itself**?

Correct!

- (selected) Penetration Testing
- Honeypots
- Least Privileged Access Control
- Centralized Logging

Quiz Score: **13** out of 13