Knowledge Check Quiz Case Study Week 6 (Target)

Due Feb 27 at 11:59pm **Points** 15 **Questions** 15
Available until Feb 27 at 11:59pm **Time Limit** None

Instructions

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

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	7 minutes	15 out of 15

Score for this quiz: **15** out of 15
Submitted Jan 24 at 11:54am
This attempt took 7 minutes.

Question 1 — 1 / 1 pts

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

- Power Grid
- Bank
- Credit Card Information — Correct!
- Energy Sector

Question 2 — 1 / 1 pts

Where did the attack occur?

- Ukraine
- Iran

Correct!

- (selected) United States
- Australia

Question 3

1 / 1 pts

What was the **duration** of this attack from initiation to discovery?

Note: Duration for this question is from attack initiation to discovery and does not include the phishing campaign.

Correct!

- (selected) 3 Weeks
- 3 Years
- 3 Hours
- 3 Days

Question 4

1 / 1 pts

When was the attack **discovered**?

- April 2007

Correct!

- (selected) December 2013
- March 2011
- August 2014

Question 5

1 / 1 pts

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

- Corporate secrets stolen
- Widespread power outages
- Centrifuges were destroyed

Correct!

- (selected) Credit card information stolen

Question 6

1 / 1 pts

What makes this case study **significant**?

- Denial of service attack as cyber warfare
- Insider attack on industrial control systems
- Malware introduced to critical infrastructure

Correct!

- (selected) Wide spread attack on credit card terminals

Question 7

1 / 1 pts

How did the attack occur?

- Malware introduced in firmware updates
- Phishing campaign to gain credentials

Correct!

- Distributed denial of service attack on government websites
- Radio signals to SCADA devices causing pumps to fail

Question 8

1 / 1 pts

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

- Adobe Flash vulnerability used to inject malicious code
- PING flood and botnets
- SCADA system insecure
- RAM scraping malware installed on Point of Sale terminals

Correct!

Question 9

1 / 1 pts

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

- Security team ignored warnings from anti-intrusion system

Correct!

- Contractor USB sticks used to install malware
- Coordinated cyber attack as political protest
- Disgruntled employee sabotaged operations

Question 10

1 / 1 pts

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

- Heavy dependence on IT services
- Failed to isolate sensitive network assets
- Old versions of Office and Windows
- Vendor with weak security practices given access

Correct!

Question 11

1 / 1 pts

The HVAC employees needed access to the Target billing system to process their invoices. They did not need access to the Point of Sale systems, but they were connected. When an HVAC employee responded to a phishing email, the **malware spread from the billing system to the Point of Sale system**. What **vulnerability** does this represent?

- Security patches not installed
- Two-factor authentication disabled on internal servers
- Failed to isolate sensitive network assets

Correct!

- Old operating systems on ICS networks

Question 12

1 / 1 pts

Which **malware** was used in the attack?

- Black Energy
- Black POS

Correct!

- Poison Ivy
- Stuxnet

Question 13

1 / 1 pts

In which phase of the **Intrusion Kill Chain** did the attacker **identify Fazio as Target's HVAC vendor**?

- Installation
- Actions on Objective
- Reconnaissance

Correct!

- Weaponization

Question 14

1 / 1 pts

In which phase of the **Intrusion Kill Chain** did the attacker **send infected emails to Fazio in a phishing attack**?

Correct!

- (selected) Delivery
- Command & Control
- Reconnaissance
- Actions on Objective

Question 15

1 / 1 pts

In which phase of the **Intrusion Kill Chain** did **RAM scraping malware begin recording card swipes**?

- Command & Control
- Reconnaissance

Correct!

- (selected) Exploitation
- Weaponization

Quiz Score: **15** out of 15