Knowledge Check Quiz Case Study Week 10 (Dyn)

Due Mar 27 at 11:59pm **Points** 10 **Questions** 10
Available until Mar 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	less than 1 minute	10 out of 10

Score for this quiz: **10** out of 10
Submitted Jan 31 at 11:45am
This attempt took less than 1 minute.

Question 1 — 1 / 1 pts

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

- Bank
- Power Grid
- Water Services
- Correct! Internet

Question 2 — 1 / 1 pts

Where did the attack start?

Correct!

- (selected) United States
- Iran
- Estonia
- Australia

Question 3

1 / 1 pts

When did this attack occur?

- June 2010
- December 2015

Correct!

- (selected) October 2016
- April 2000

Question 4

1 / 1 pts

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

- Credit card information stolen

Correct!

- (selected) Internet sites not available or sluggish
- Widespread power outages

Corporate secrets stolen

Question 5

1 / 1 pts

What makes this case study **significant**?

Malware introduced to power grid

Wide spread attack on credit card terminals

Insider attack on industrial control systems

Correct!

Denial of Service attack using IoT devices

Question 6

1 / 1 pts

How did the attack occur?

Phishing campaign to introduce malware

Supply chain attack on Industrial Control Systems

Hackers stole credentials from HVAC vendors

Correct!

DDoS attack on DNS provider

Question 7

1 / 1 pts

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

- RAM scraping malware installed on Point of Sale terminals
- Correct! IoT devices infected with malware
- SCADA system not secure
- VPNs lacked 2-factor authentication

Question 8

1 / 1 pts

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

- Employee opens attachment on phishing email
- Correct! Consumers kept default passwords
- Contractor USB sticks used to install malware
- Disgruntled employee sabotaged operations

Question 9

1 / 1 pts

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

- Old versions of Office and Windows
- Two-factor authentication disabled on internal servers

Correct!

- (●) Vendors not competing to create secure products
- ( ) Workarounds to address problem equipment masked attack

Question 10

1 / 1 pts

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

- ( ) Poison Ivy
- ( ) Stuxnet

Correct!

- (●) Mirai
- ( ) Havex

Quiz Score: **10** out of 10