Knowledge Check Quiz Case Study Week 2 (Maroochy)

Due Jan 30 at 11:59pm **Points** 15 **Questions** 15
Available until Jan 30 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 17 at 10:46am
This attempt took 7 minutes.

Question 1

1 / 1 pts

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

○ Power Grid

○ Fuel Enrichment Plant

Correct! ● Water Services

○ Bank

Question 2

1 / 1 pts

Where did the attack occur?

○ Estonia

○ Ukraine

○ United States

Correct! ● Australia

Question 3

1 / 1 pts

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

○ 3 days

Correct! ● 3 months

○ 3 weeks

○ 3 hours

Question 4

1 / 1 pts

When was the attack **discovered**?

○ April 2014

○ July 2010

Correct!

● April 2000

○ December 2015

Question 5

1 / 1 pts

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

○ Corporate secrets stolen

Correct!

● Raw sewage was spilled

○ Credit card information stolen

○ Widespread power outages

Question 6

1 / 1 pts

What makes this case study **significant**?

○ Supply chain attack on industrial control systems

Correct!

● Insider attack on industrial control systems

○ Denial of service attack on critical infrastructure

○ Malware introduced to critical infrastructure

Question 7

1 / 1 pts

How did the attack occur?

○ Malware introduced in firmware updates

Correct! ● Radio signals to SCADA devices causing pumps to fail

○ Distributed denial of service attack on government websites

○ Phishing campaign to gain credentials

Question 8

1 / 1 pts

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

○ Malware designed to impose damage

○ PING flood and botnets

○ Adobe Flash vulnerability used to inject malicious code

Correct! ● SCADA system insecure

Question 9

1 / 1 pts

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

○ Employees open attachment on phishing email

Correct! ● Disgruntled employee sabotaged operations

○ Contractor USB sticks used to install malware

○ Security team ignored warnings from anti-intrusion system

Question 10

1 / 1 pts

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

○ Two-factor authentication disabled on internal servers

Correct!

● Subcontractor with weak security practices given access

○ Security patch not installed

○ Old versions of Office and Windows

Question 11

1 / 1 pts

What does the acronym **SCADA** stand for?

○ System Commands and Defined Accounts

Correct!

● Supervisory Control and Data Acquisition

○ Security Communications and Distributed Access

○ Segment Cyber and Denial Actions

Question 12

1 / 1 pts

Who was the disgruntled employee that posed the insider threat?

○ Robert Stringfellow

○ Hunter Watertech

○ Steve Yager

Correct! ◉ Vitek Boden

Question 13

1 / 1 pts

What does the acronym **ICS** stand for?

○ Interactive Communication Services

○ Intentional Carrier Sequence

○ Identity Cyber Security

Correct! ◉ Industrial Control System

Question 14

1 / 1 pts

Which was a **fault** experienced by the system as a result of the attack?

○ Pumps operated at speeds that caused them to fail

Correct! ◉ Pumps were not running when they should have been

○ Customer complaints overwhelmed the company switchboard

○ False alarms caused the operators to ignore failures

Question 15

1 / 1 pts

What does the acronym **PLC** stand for?

○ Priority Landing Card

○ Private Line Carrier

○ Primary Link Communications

Correct!

● Programmable Logic Controller

Quiz Score: **15** out of 15