2021 CASE
Fast version

Dean Bushmiller CISSP+32

Case Progression

Students read short case

Students propose business problem

Dean picks best 2 problems

Students solve problem in CISSP way

Dean defines best solutions & critiques

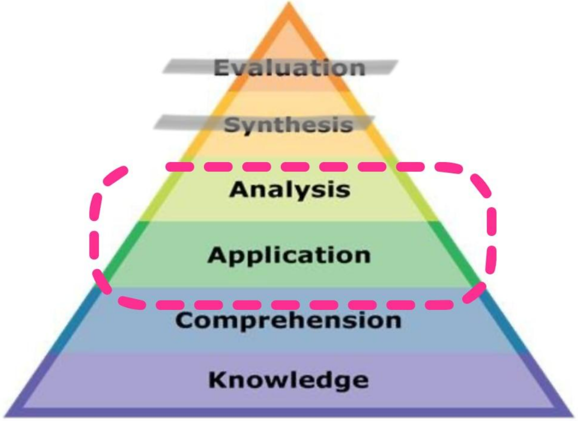
Why Cases?

Exam requires 40-50% Analysis

This activity is how you build analysis skill

Analysis is your job as a CISSP

No one is good at analysis without practice



EXAM QUESTION – WHY YOU LEARN WITH CASES

The Company is reviewing its virtual private network (VPN) strategy. Its current vendor has a proprietary encryption protocol in place based on the Data Encryption Standard (DES). The one main office has a 1.5Mb connection to the Internet. It has 200 remote users on a variety of operating systems platforms. The primary uses for the remote users are order entry, timesheet reporting, and online meetings. The company has 1,000 clients that connect to the intranet for a custom order entry solution. Clients use the HTTPS protocol and a fixed password per account. They are willing to replace the current solution if a cost-effective alternative is available. The Company priorities' are security of remote connections and client connectivity.

Which of the following is best for high-speed remote access that uses VPNs?

A. TLSv1.3 with ISDN
B. Cable modems with DSL
C. Modem pools with DSL
D. IPSec with ISDN

Cases in context = Exam Question

Who are you representing?

- Organization / Mission
- NOT individual

What is your role?

- Chief Information Security Officer
- NOT technician

What are your limits?

- BIGGEST WIDEST ANSWER for all
- NOT technical solution

This activity works well for 40% of exam questions

- 10-20% Scenario questions

Case Practice

Get a feel & ask questions

For skill building we will stay in ONE domain

When learning

- you cannot do all at once
- You will be tempted to go with what you know

DIFFERENT LEVELS / TRY ALL BUT KNOW YOU ARE STRETCHING

DO NOT JUMP AHEAD TO SOLUTION

All done by you in BLUE FORM

1. E – Read
2. E – Set Domain & Terms
3. E – List the core principle that is violated
4. E – Identify decision makers **(more next)**
5. I – Define business problems
6. I – List value at risk
7. I – Propose solution as sentence
8. A – Question can you ask for engagement

Entry:

Intermediate:

Advanced:

Which of these is a CISSP decision maker? (Q&A w/#)

1. User
2. Help Desk
3. Incident response
4. Business partner
5. Vendor
6. Customer
7. Auditor
8. Board of directors
9. C–level
10. CISO
11. Human resources
12. Legal
13. Regulators

BIGGEST MISTAKE "LACK OF X" IS NOT A PROBLEM

"The problem is a lack of security/ firewall/ policy"

- That is the solution.
- That make this YOUR problem to solve.

By stating the problem *without the solution*

- You analysis skill is much stronger
- You technical stuff looks like a small part of problem

BEST way define

- RISK to business with impact on whole business

We are here to analyze Management of Security