CISM Domains

CISM is divided into four domains.

Domain 1: Information Security Governance.

Domain 2: Information Security Risk Management.

Domain 3: Information Security Program Development and Management.

Domain 4: Information Security Incident Management.

CASE STUDY

Colonial Pipeline Hack

Colonial Pipeline Cyber Attack - 2021

Colonial Pipeline is one of the largest pipeline operators in the United States

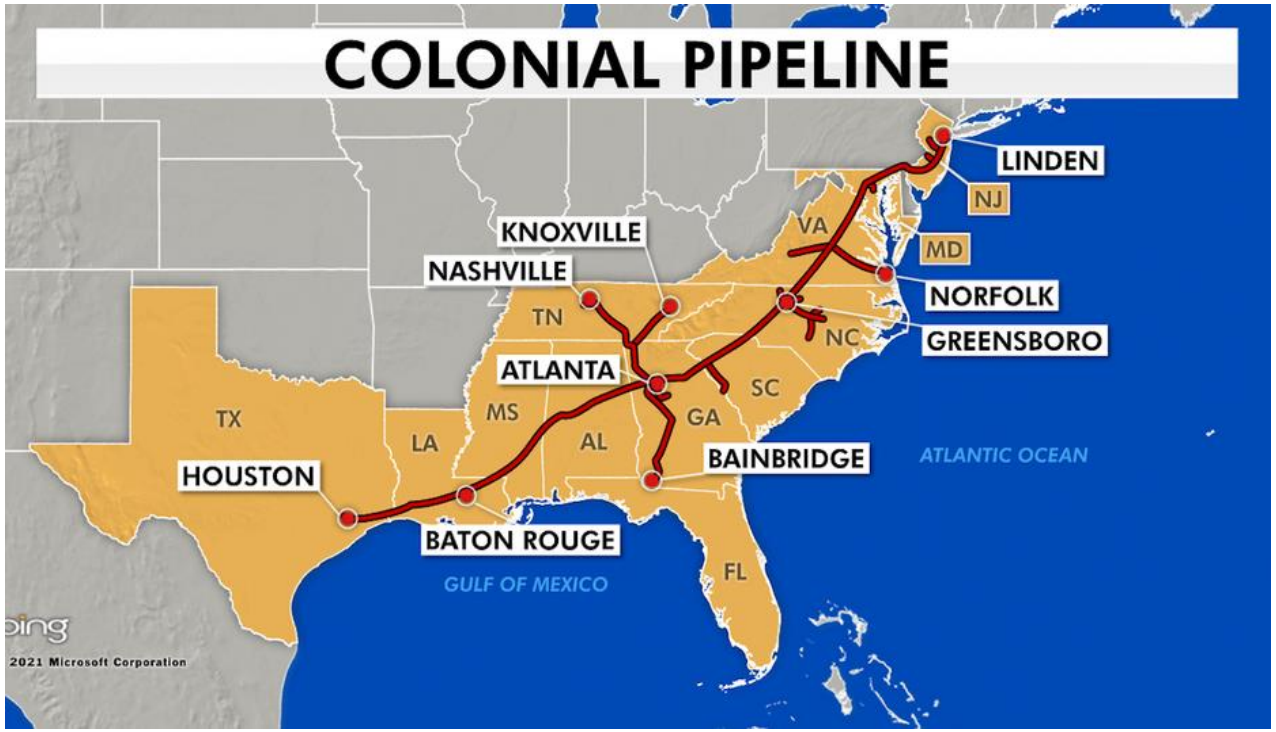
Attack:

Colonial Pipeline suffered a ransomware attack that forced the U.S. energy company to shut down its entire fuel distribution pipeline.

May 6, 2021: Malicious actors launch an attack, stealing data, locking computers, and requesting a ransom.

Who did this:

A hacker group called DarkSide, which is set up as a "ransomware as a service" business model, is reportedly behind the cyberattack.



$ 5 Million Ransom paid

Attack Vector

Attackers got into the Colonial Pipeline network through an exposed password for a VPN account.

Technical Details:

DarkSide actors have previously been observed gaining initial access through phishing and exploiting remotely accessible accounts.

- Exploit Public-Facing Application
- External Remote Services
- Remote Desktop Protocol

Problem:

- OT and ICS running on an older vulnerable platform.
- Patches for vulnerable software are often simply not available.

Attack Vector

The attack vector is the same in 2021 as it was in 2012.

Hillary Clinton’s Email Was Probably Hacked, Experts Say

Ref:

https://www.nytimes.com/2016/07/07/us/hillary-clintons-email-was-probably-hacked-experts-say.html
https://www.reuters.com/article/us-clinton-emails-hacker-idUSKCN0YF2KZ
https://www.bbc.com/news/world-us-canada-31806907

One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

Ref:

https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html
https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?leadSource=uverify%20wall

CISM Aspect

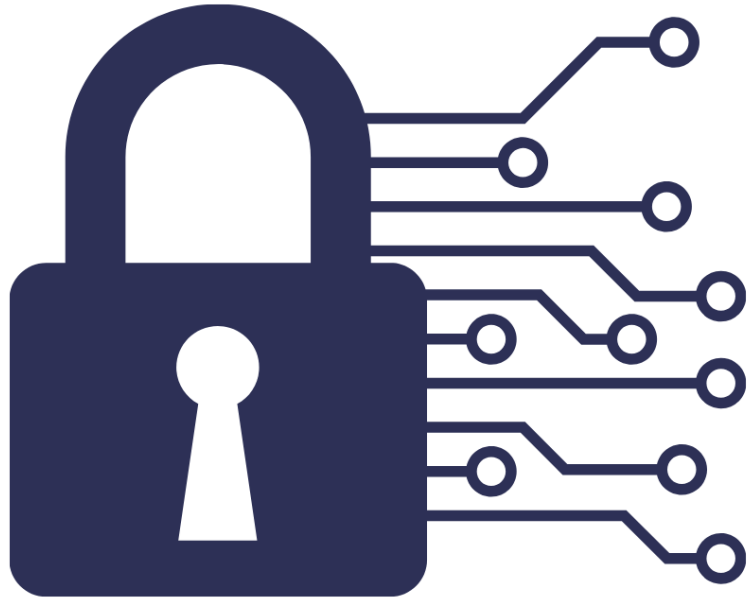
- Discover your attack surface and automated comprehensive asset inventory list.
- Conduct regular security assessments
- Introduce End Of Life (EOL) Policy to handle non-available patch solutions
- Periodic security awareness training for employees because they are the last line of defense and primary attack vector for hackers.
- Implement the principle of least privileges - Access Management.
- Implement multi-factor authentication.
- Enable strong spam filters.
- Limit access to resources over the network, especially restricting Remote Desktop Protocol(RDP).
- Build zero-trust architecture.
- Organize OT assets into logical zones and monitor traffic between zones.
- Implement data backup and ensure backup regularly tested.

Contingency Plan

- **Prepare**
- **Analyze**
- **Develop**
- **Implement**
- **Review**

The same we will be studying in CISM:

- Information Security Governance
- Information Risk Management
- Information Security Program Development and Management
- Information Security Incident Management



Domain 1

Information Security Governance

Pre-Course Question 1

A security strategy is important for an enterprise **PRIMARILY** because of it:

A. provides a basis for determining the best logical security architecture.
B. provides the approach to achieving the outcomes management wants.
C. provides users guidance on how to operate securely in everyday tasks.
D. helps IT auditors ensure compliance with rules and regulations.

Pre-Course Question 1

A security strategy is important for an enterprise **PRIMARILY** because of it:

A. provides a basis for determining the best logical security architecture.
B. provides the approach to achieving the outcomes management wants.
C. provides users guidance on how to operate securely in everyday tasks.
D. helps IT auditors ensure compliance with rules and regulations.

Correct Answer is B.

A security strategy will define the approach to achieving the security program outcomes management wants. It should also be a statement of how security aligns with and supports business objectives. It provides the basis for good security governance.

Pre-Course Question 2

Which of the following is the MOST important reason to provide effective communication about information security?

A. It makes information security' more palatable to resistant employees.
B. It mitigates the weakest link in the information security landscape.
C. It informs business units about the information security strategy.
D. It helps the enterprise conform to regulatory information security requirements.

Pre-Course Question 2

Which of the following is the MOST important reason to provide effective communication about information security?

A. It makes information security' more palatable to resistant employees.
B. It mitigates the weakest link in the information security landscape.
C. It informs business units about the information security strategy.
D. It helps the enterprise conform to regulatory information security requirements.

Correct Answer is B.

Security failures are, in the majority of instances, directly attributable to lack of awareness or failure of employees to follow policies or procedures. Communication is important to ensure continued awareness of security policies and procedures among staff and business partners.

Part A

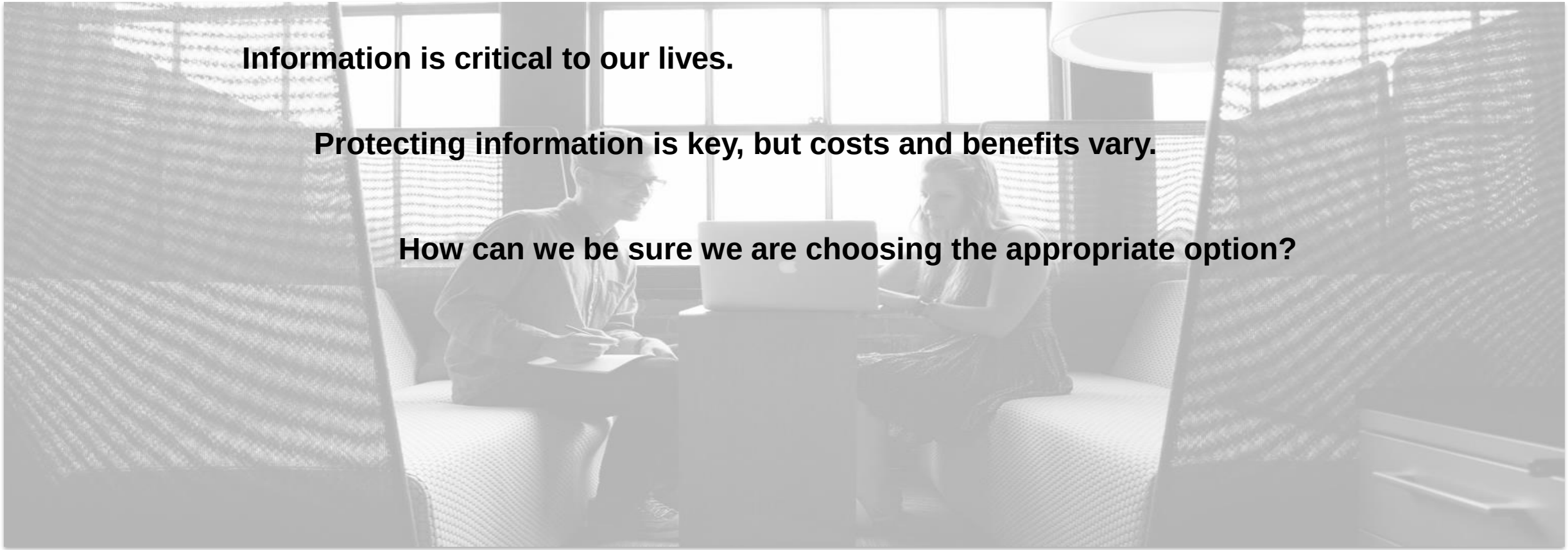
Enterprise Governance

Governance vs. Management

- Governance
  - Purpose is to set goals
  - “Do the right thing”

- Management
  - Purpose is plan, build, execute and monitor activities to achieve goals
  - “Do the thing right”

Why Does Governance Matter?



- Governance helps align information security with business goals and objectives