Audit Planning - Scenario

- You are planning an IS audit for a financial services company specializing in synthetic financial derivatives
- The focus of the audit will be compliance with financial industry regulations
- Auditors may be exposed to sensitive financial data

Audit Planning

- Which recommendations should be made *prior* to conducting the IS audit?

Audit Planning - Answer

- Make sure you understand the nature of the business and its processes
- Existing company documentation should be acquired
- Ask if a recent risk assessment has been conducted
- A Non Disclosure Agreement (NDA) should be created and signed

Security Control Cost Effectiveness - Scenario

- Your client gathers market research data that it then sells to marketing firms
- The market research databases are valued at $250,000
- A single security breach could cost up to $10,000
- Security breaches are estimated to occur once every 36 months

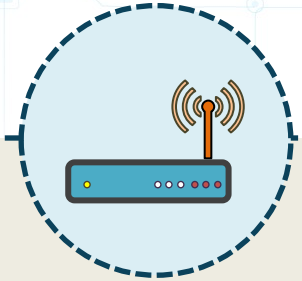
Security Control Cost Effectiveness

- You estimate that protecting the marketing research databases has an annual cost of $2,600
- Should you invest in protecting the databases at this cost?

Security Control Cost Effectiveness - Answer

- Yes, invest in protecting the databases at an annual cost of **$2,600**
- Annual Loss Expectancy (ALE)
  - Single Loss Expectancy x Annual Rate of Occurrence
  - $10,000 x .333 = **$3,330**

Wi-Fi Security Recommendations - Scenario



- Your client has installed a Wi-Fi router in the executive boardroom
- Wi-Fi will be used to allow Internet access
- The SSID name is set to "Executive Boardroom"
- WPA2 PSK has been configured
- The Wi-Fi router is plugged into the same Ethernet switch as corporate servers

Wi-Fi Security Recommendations

- Your client has ecommerce websites on the corporate network
- The ecommerce sites process payments using customer credit cards
- Which Wi-Fi security recommendations would you make?

Wi-Fi Security Recommendations - Answer

- If boardroom attendees are using laptops, consider using wired network connections
- Change the SSID to a generic name
- Ensure the Wi-Fi router is plugged into a switch for public-facing connections only
- Configure RADIUS authentication and Network Access Control (NAC)

Travelling Users and Security - Scenario

- During your IS audit you uncover a pattern of data privacy incidents stemming from travelling users
- Some users log into computers in the hotel guest office to access corporate data and copy it to a USB thumb drive
- Travelling users sometimes went two months before receiving any type of software updates

Travelling Users and Security

- You need to make recommendations to ensure travelling users work in a more secure fashion
- Which recommendations can result in reduced risk?

Travelling Users and Security - Answer

- More frequent user awareness training
- More up-to-date security policy documentation
- Security policies made easily available on Intranet website
- Implement a data loss prevention (DLP) solution
- Prevent the use of USB thumb drives
- Implement a remote VPN solution that is active prior to user logon

Key Usage - Scenario

- Users complain that when they attempt to send encrypted e-mail messages to a specific user, an error message states that the message cannot be encrypted
- Executives ask you to recommend a solution so that e-mail messages received from departmental managers are assured to be authentic

Key Usage - Answer

- Encrypting an e-mail message uses the *public* key of the *recipient*; verify the key is available and not expired
- Digitally signing an e-mail message occurs using the *sender's private* key
- Message validation occurs by the recipient using the *sender's public* key

Suggest Compensating Controls

Requirement	Compensating Control
Prevent unwanted network access	
Segregation of duties	
Multifactor authentication for each application	

Suggest Compensating Controls

Requirement	Compensating Control
Prevent unwanted network access	Disable unused switch ports
Segregation of duties	Video surveillance
Multifactor authentication for each application	Network access control with multifactor authentication

In this exercise, you will

- Describe the relationship between IS auditing and risk management
- Describe how intersecting risk between Wi-Fi security and IT technicians can be managed
- Describe how public and private keys are used
- Describe when compensating controls should be used

IS Auditing and Risk Management

- IS auditing strives to identify threats to assets and manage that risk
  - Risk acceptance
  - Risk transfer
  - Risk reduction

Wi-Fi Security and IT Technicians

- Proper change and configuration management processes and approvals
- Thorough IT technician background checks prior to hiring

Public and Private Keys

- They are mathematically related and issued to user, app, or device
- Encrypting messages uses the recipient's public key (decryption uses the recipient's private key)
- Digitally signing messages uses the sender's private key (verification uses the sender's public key)

Compensating Control Usage

- Use as an alternative to the ideal desired control
- Ideal desired control
  - Implementation too difficult
  - Too costly