Q.1 A Business Trip to South America Goes South

SCENARIO: A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originating from South America. There was an additional $1,000 overdraft fee.

ATTACK: The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

What is Skimming? Skimming occurs when criminals install devices on ATMs, point-of-sale (POS) terminals, fuel pumps, etc. to capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts.

RESPONSE: Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's personal account.

The firm severed ties with that bank. The new bank offered comprehensive fraud protection guarantees. The firm created two business accounts:

- one for receiving funds and making small transfers
- one for small expense payments

The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically,

pay cash, or use a major credit card, as necessary.

IMPACT: The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

LESSONS LEARNED:

1. Use major credit cards when traveling - they have more consumer fraud protection than debit cards.
2. Get notified - set up transaction alerts with your credit and debit card companies to monitor fraud.
3. Check your bank account frequently.
4. Create withdrawal alerts.
5. Understand your bank's policies about covering losses from fraud.

DISCUSS:

1. Knowing how the firm responded, what would you have done differently? (2.5 Marks)
2. What are some steps you think the firm could have taken to prevent this incident? (2.5 Marks)
3. Is your business susceptible? How are you going to reduce your risk? (2.5 Marks)

⇨ Knowing how the firm responded, what would you have done differently? Considering the scenario, there are a few steps that could have been taken differently:

1. Educating Employees: Prior to the business trip, the consulting firm could have provided training or information to employees about the risks associated with using debit cards at unfamiliar ATMs, especially in regions known for skimming incidents. This would raise awareness and help employees make more informed decisions.
2. Implementing Travel Policies: The firm could have established clear travel policies that explicitly prohibit the use of company-provided debit cards in high-risk areas or at unfamiliar ATMs. This would ensure that employees are aware of the risks and alternative payment methods.

3. Enhanced Monitoring and Notifications: The firm could have set up additional monitoring measures, such as transaction alerts and withdrawal notifications, on the business account used for travel expenses. This would enable them to detect any fraudulent activity promptly and take immediate action.

What are some steps you think the firm could have taken to prevent this incident? To prevent such incidents in the future, the firm could have taken the following steps:

1. Use Secure Payment Methods: Instead of relying on debit cards, the firm could have encouraged employees to use secure payment methods, such as major credit cards, which generally offer better fraud protection and easier reimbursement processes.
2. Enable Travel Expense Prepayment: The firm could have implemented a system where employees prepay their travel expenses electronically through the firm's account. This would eliminate the need for employees to use their personal cards or withdraw cash during the trip.
3. Utilize Virtual Cards: The firm could have explored the use of virtual cards or virtual payment solutions specifically designed for business travel. Virtual cards provide additional security as they generate unique card numbers for each transaction, reducing the risk of unauthorized use.

Is your business susceptible? How are you going to reduce your risk? To assess the susceptibility of your business to similar incidents and reduce the risk, consider the following steps:

1. Evaluate Payment Practices: Review the payment methods used by your business for travel expenses or any other transactions involving financial cards. Identify areas where the use of debit cards or other vulnerable payment methods may pose risks and consider alternative, more secure options.
2. Implement Security Awareness Training: Educate employees about common fraud techniques, such as skimming, phishing, or social engineering, and provide guidelines on secure payment practices. Promote a culture of security awareness to ensure employees make informed decisions.
3. Strengthen Payment Controls: Implement strong payment controls, such as transaction monitoring, alerts, and limits, to identify suspicious or unauthorized activity promptly. Regularly review and reconcile financial statements to detect any anomalies or discrepancies.
4. Use Multi-Factor Authentication: Enable multi-factor authentication (MFA) for financial accounts and ensure employees use strong, unique passwords. MFA adds an extra layer of protection by requiring additional verification beyond just a password.
5. Regularly Review and Update Policies: Periodically review and update your organization's policies related to payment methods, expense reimbursement, and travel protocols to incorporate best practices and address emerging risks.

By adopting these measures, businesses can reduce their susceptibility to fraud and enhance their overall security posture when it comes to financial transactions and travel-related expenses.

Q.2 What distinguishes an access control list from a capability ticket in terms of their purpose and implementation in computer security?

=> Access Control List (ACL) and Capability Ticket are two different access control mechanisms used in computer security. Here's how they differ in terms of purpose and implementation:

Access Control List (ACL):

1. Purpose: An ACL is a list or table that defines permissions and access rights for individual users or groups. It specifies who is allowed or denied access to specific resources or objects in a system.
2. Implementation: ACLs are typically associated with the resources themselves, such as files, directories, or network shares. They are maintained by the operating system or a security subsystem. Each entry in the ACL contains a subject (user or group) and the associated permissions (read, write, execute, etc.). When a user requests access to a resource, the ACL is consulted to determine whether the requested action is allowed.

Capability Ticket:

1. Purpose: A capability ticket is a token or key that grants specific privileges or access rights to a user or process. It is essentially a proof of authorization that can be presented to the system or other entities to gain access to resources.
2. Implementation: Capability tickets are typically implemented as unforgeable tokens, often containing cryptographic elements. They are generated by a trusted authority and associated with specific permissions or capabilities. When a user or process presents a capability ticket, the system checks its validity and the associated privileges before granting access to the requested resource.

In summary, the key distinctions between ACL and Capability Ticket are as follows:

1. Scope: ACLs focus on defining access rights at the resource level, while Capability Tickets grant privileges to specific users or processes.
2. Association: ACLs are typically associated with resources themselves, while Capability Tickets are separate entities granted by a trusted authority.
3. Access Control: ACLs are consulted at the time of access request to determine permissions, while Capability Tickets are presented as proof of authorization.
4. Authorization Model: ACLs follow the discretionary access control (DAC) model, where owners control access to their resources. Capability Tickets are often associated with

the mandatory access control (MAC) model, where privileges are assigned by a central authority.

Both ACLs and Capability Tickets have their uses in different security scenarios, and the choice of which mechanism to use depends on the specific requirements and design of the system.

Q.3 **What are some examples of administrative policies that can be implemented in a relational database management system, and what is the purpose of each policy?**

=> In a relational database management system (RDBMS), various administrative policies can be implemented to govern the behavior and operations of the system. Here are some examples of such policies and their purposes:

1. Password Policy: This policy defines the rules and requirements for user passwords, such as complexity, length, expiration, and reuse restrictions. Its purpose is to enforce strong security practices and protect the system from unauthorized access.
2. Backup and Recovery Policy: This policy outlines the procedures and schedules for backing up the database and recovering data in case of system failures, disasters, or human errors. Its purpose is to ensure data availability, integrity, and minimize downtime.
3. Data Retention Policy: This policy specifies the duration for which data should be retained in the database before it is purged or archived. Its purpose is to comply with legal, regulatory, or business requirements related to data retention and to manage storage efficiently.
4. Access Control Policy: This policy governs the granting and revocation of user privileges and permissions within the database. It determines who can perform specific actions, access certain data, or modify the database structure. Its purpose is to maintain data confidentiality, integrity, and prevent unauthorized activities.
5. Auditing Policy: This policy defines the extent of database activity logging, including what actions should be recorded, how long logs should be retained, and who has access to audit trails. Its purpose is to monitor and track user actions, detect security breaches, ensure accountability, and facilitate forensic investigations if needed.
6. Performance Tuning Policy: This policy outlines guidelines and best practices for optimizing the performance of the database system. It covers areas such as index creation, query optimization, disk allocation, and resource allocation. Its purpose is to enhance system responsiveness, scalability, and user experience.
7. Data Archiving Policy: This policy governs the process of moving less frequently accessed or historical data to separate storage, such as an archival database or offline storage. Its purpose is to free up resources, improve performance, and facilitate efficient management of active data.

8. Data Privacy Policy: This policy establishes guidelines and protocols for handling sensitive or personally identifiable information (PII) within the database. It addresses aspects like data encryption, anonymization, and compliance with privacy regulations. Its purpose is to protect individuals' privacy and ensure compliance with legal requirements.
9. Change Management Policy: This policy defines the procedures and approvals required for making changes to the database structure, configurations, or software versions. Its purpose is to maintain system stability, minimize disruptions, and ensure proper documentation of changes.
10. Disaster Recovery Policy: This policy outlines the strategies and protocols for recovering the database and resuming operations after a catastrophic event or major system failure. It includes backup procedures, replication mechanisms, and failover plans. Its purpose is to minimize data loss, maintain business continuity, and reduce downtime.

These are just a few examples of administrative policies that can be implemented in an RDBMS. The specific policies and their purposes may vary depending on the organization, its requirements, and the nature of the database system being used.

Q.4 **What are the advantages and disadvantages to database encryption?**

=> Database encryption offers several advantages and disadvantages. Let's explore them:

Advantages of Database Encryption:

1. Data Confidentiality: Encryption ensures that sensitive data remains confidential and unreadable to unauthorized individuals or entities. Even if the database is compromised, encrypted data is protected.
2. Compliance with Regulations: Encryption is often a requirement for compliance with various data protection regulations and industry standards. By encrypting data, organizations can demonstrate their commitment to safeguarding sensitive information.
3. Protection against Insider Threats: Encryption helps mitigate risks associated with insider threats. Even authorized users with access to the database cannot view the encrypted data without proper decryption keys, reducing the potential for misuse or unauthorized disclosure.
4. Secure Data in Transit: When data is encrypted at the database level, it remains encrypted during transmission. This ensures the security and integrity of the data when moving between different systems or over untrusted networks.
5. Defense against Data Breaches: In the event of a data breach, encrypted data is significantly more difficult to exploit. Encryption raises the bar for attackers, as they

would need to bypass encryption measures to access the sensitive information stored in the database.

Disadvantages of Database Encryption:

1. Performance Overhead: Encryption and decryption processes can introduce additional computational overhead, which may impact the performance of database operations. The processing power required for encryption can result in increased response times and resource utilization.
2. Key Management Complexity: Encryption requires robust key management practices. Organizations must securely store and manage encryption keys, ensuring their availability and protecting them from unauthorized access. Effective key management can be challenging and requires careful planning.
3. Increased Storage Requirements: Encrypted data tends to be larger in size compared to its unencrypted counterpart. This increase in storage requirements can impact the overall storage capacity and costs of the database system.
4. Limited Searchability: Encrypted data is not easily searchable unless a specialized search technique called homomorphic encryption is used. Traditional encryption techniques hinder the ability to perform complex queries or search operations on encrypted data directly.
5. Impact on Database Functionality: Encryption can affect certain database features and functionality. For example, encrypted data may not be usable in some database operations, such as indexing or sorting, which heavily rely on the ability to manipulate data in plaintext form.

It is important to carefully consider the specific requirements and trade-offs when deciding to implement database encryption. Organizations must weigh the benefits of increased security and compliance against the potential performance impact and added complexity of managing encryption keys. Additionally, a comprehensive security strategy should include encryption alongside other security measures to provide layered protection for the database and the overall data ecosystem.

Q.5 **Describe some malware countermeasure elements?**

=>To counteract malware and enhance overall security, several countermeasure elements can be implemented. Here are some common ones:

1. Antivirus/Antimalware Software: Deploying antivirus or antimalware software is crucial to detect, prevent, and remove known malware threats. These software solutions typically employ signature-based detection, behavioral analysis, heuristics, and real-time scanning to identify and eliminate malicious code.

2. Firewall: A firewall acts as a barrier between an internal network and external networks, controlling incoming and outgoing network traffic based on predetermined security rules. It helps block unauthorized access and prevents malware from infiltrating the network.
3. Intrusion Detection and Prevention Systems (IDS/IPS): IDS/IPS solutions monitor network traffic and system activity for suspicious or malicious behavior. They can detect and alert administrators about potential malware attacks or intrusion attempts and may even block or mitigate them in real-time.
4. Security Patch Management: Regularly applying security patches and updates to the operating system, applications, and firmware is essential. These patches address known vulnerabilities that malware often exploits. Prompt patch management minimizes the attack surface and reduces the chances of successful malware infections.
5. User Education and Awareness: Educating users about safe computing practices and raising awareness about malware threats are vital countermeasures. Users should be trained to recognize phishing emails, avoid suspicious downloads or websites, and exercise caution while opening attachments or clicking on links.
6. Secure Configuration: Implementing secure configurations for operating systems, applications, and network devices helps minimize vulnerabilities. This includes disabling unnecessary services, configuring proper access controls, using strong passwords, and applying the principle of least privilege.
7. Data Backup and Recovery: Regularly backing up critical data and ensuring proper backup storage is an effective countermeasure against malware attacks. In case of infection or data loss, a recent backup allows for recovery without paying ransom or suffering from permanent data loss.
8. Web Content Filtering: Web content filtering solutions block access to malicious or inappropriate websites, preventing users from inadvertently downloading malware or accessing harmful content. Filtering can be based on categories, reputation lists, or specific policies.
9. Email Filtering: Deploying email filtering mechanisms can help block or quarantine suspicious emails, including those carrying malware-laden attachments or malicious links. Advanced email filters use spam detection, antivirus scanning, and machine learning techniques to identify and mitigate threats.
10. Network Segmentation: Segmenting the network into isolated zones and implementing proper access controls restricts lateral movement of malware. If one segment gets infected, the spread of malware to other segments is limited, minimizing the potential impact.

These countermeasure elements, when implemented in a layered defense strategy, significantly enhance an organization's ability to prevent, detect, and mitigate malware threats. It's important to regularly update and maintain these countermeasures to stay ahead of evolving malware techniques.