Written-Response questions:

**1.**

**a.**

Integrity.

The integrity is violated because in this case, the accuracy and trustworthiness of the data can not be maintained. Since the machine could change the voting result without letting anyone notice (may altered by unauthorized people). I think the integrity is compromised.

**b.**

Availability and Integrity

In this case the availability is affected. The voting stations should be easy and convenient for all people to access, but by moving the station from the easy access locations for certain voters, the availability of the voting station is violated. Since it becomes harder for certain demographics of voters to vote, the integrity of the voting system is also compromised. Because the inconvenience may cause some people not going to vote which leads to inaccuracy and not trustworthy result.

**c.**

Confidentiality

In this scenario, the confidentiality of the voting system is compromised since the some of the voting machine had internet access and already been accessed by unauthorized people. Letting sensitive information accessed by unauthorized people is violating confidentiality.

**d.**

Integrity

Since the false information has been distributed, there is a chance that the information has an influence on voters which may lead them to vote for the person they were not intend to vote for. This scenario will compromise the accuracy and trustworthiness of the voting result which compromise the integrity.

**2.**

**a.**

**Modification:**

Since the emails should always be retained in the public interest and some of them are missing and incomplete, there must have been some unauthorized people/party had accessed and tampered the data. So it is an modification threat.

**b.**

**Fabrication:**

The video is not real and modified using “Deep Fake” which is used to have a bad negative impact on the political opponent. So this is a fabrication threat.

**c.**

**Interruption:**

The agents stopped us from accessing the bank domain, which means the asset is unavailable for us and this is interruption.

**d.**

**Interception:**

The phone call content should be securely transferred between caller and receiver. But in the case the agent may have wiretapped to obtain the conversation and it mean the unauthorized party has gained access to an asset which is interception.

3.

**Preventing:**

Disconnect all voting machines from the internet. Remove the NICs previously found in some of the machines. Lock the machines to prevent unauthorized modification.

**Detecting:**

Add a physical detector and alarm within the voting machine. The alarm will go on if any voter try to perform action that is not allowed or any unauthorized people try to access the machine.

**Recovering:**

Keep all the physical votes records secure and complete, to use it to recount the voting result if anything happens to the voting machine or you believe the machines have been compromised.

4.

**Signature-based analysis:**

This method uses the characteristic feature (the signature) of list of all known malware programs to search for matching data in the system.

Step 1. Analysis the three malware programs to identify its unique characteristic feature as the signature.

Step 2. Scan the voting system using the signature to find malware programs.

**Behavior-based analysis:**

This method looks for suspicious patterns of behavior, rather than for specific code fragments.

Step 1. Execute three malware programs in sandbox and analysis their behavior patterns.

Step 2. Analysis the voting machines looking for same suspicious patterns of behavior as the malware programs.