In this graduate-level scenario, we will explore a sophisticated information security breach in a banking application, focusing on breaches related to confidentiality, authenticity, and availability. Our fictional bank, SecureBank, has a reputation for robust security measures and is trusted by millions of customers worldwide. However, even the most secure systems can fall victim to highly skilled attackers.

Incident Timeline:

- Month 1: The breach begins with a highly organized cybercriminal group identifying a key vulnerability in SecureBank's external web servers through an extensive reconnaissance process. This vulnerability allows them to initiate an initial access point to the bank's network.
- Month 2: Once inside the network, the attackers exploit a zero-day vulnerability in the bank's authentication system, which allows them to escalate their privileges to gain administrative access. This breach is conducted silently to avoid detection.
- Month 3: With administrative access in hand, the attackers move laterally within the network and gain access to the highly sensitive customer database, containing personally identifiable information (PII) such as names, addresses, social security numbers, and financial transaction histories. This breach compromises the confidentiality of customer data.
- Month 4: To maintain their access and remain undetected, the attackers manipulate SecureBank's authentication system, making it appear as if they are legitimate administrators. This manipulation allows them to continue their unauthorized activities while maintaining the facade of authenticity.
- Month 5: As the breach goes undetected, the attackers decide to disrupt the availability of the banking application. They launch a distributed denial of service (DDoS) attack, flooding the bank's servers with traffic, rendering the application temporarily inaccessible to customers. This breach affects the availability of the banking services, causing panic and frustration among customers.
- Month 6: The attackers, having achieved their objectives, exfiltrate a portion of the customer data and send a ransom demand to SecureBank, threatening to release the stolen data publicly unless a significant ransom is paid in cryptocurrency. This extortion tactic puts further pressure on the bank.
- Month 7: SecureBank's security team eventually detects the breach through anomaly detection systems and the sudden availability issues. They isolate the affected systems, start incident response procedures, and engage with law enforcement agencies to investigate the breach.
- Months 8-12: The bank spends several months remediating the vulnerabilities, improving its security posture, and implementing stricter access controls. Customer data is also restored from backups, and affected customers are notified of the breach, with identity theft protection services offered.

Questions

Fill the table as discussed in the class.

No	Brief description	Type			Level of Impact (L/M/H)
		C	I	A	

- What is your understanding of Information Security w.r.t this scenario?
- Highlight the importance of continuous monitoring, timely detection, and rapid incident response in mitigating the impact of a breach.
- What was the counter measures bank adopted to minimize the risk in future.