INTERACTIVE SESSION **TECHNOLOGY**

Capital One: A Big Bank Heist from the Cloud

Capital One Financial Corporation is an American bank holding company specializing in credit cards, auto loans, banking, and savings accounts. It is the eleventh largest bank in the United States in terms of assets and an aggressive user of information technology to drive its business. Capital One was an early adopter of cloud computing and a major client of Amazon Web Services (AWS). Capital One has been trying to move more critical parts of its IT infrastructure to Amazon's cloud infrastructure in order to focus on building consumer applications and other needs.

On July 29, 2019, Capital One and its customers received some very bad news. Capital One had been breached, exposing over 140,000 Social Security numbers, 80,000 bank account numbers, tens of millions of credit card applications, and one million Canadian social insurance numbers (equivalent to Social Security numbers in the US). It was one of the largest thefts of data ever from a bank.

The culprit turned out to be Paige Thompson, a former employee of Amazon Web Services, which hosted the Capital One database that was breached. Thompson was arrested in Seattle and charged with one count of computer fraud and abuse. She had worked for the same server business that court papers said Capital One was using. Thompson could face up to five years in prison and a $250,000 fine.

The bank believed it was unlikely that Thompson disseminated the information or used it for fraud. But it will still cost the bank up to $150 million, including paying for credit monitoring of affected customers.

Amazon Web Services hosts remote servers that organizations use to store their data. Large enterprises such as Capital One build their own web applications using Amazon's cloud servers and data storage services data so they can use the information for their specific needs.

The F.B.I. agent investigating the breach reported that Ms. Thompson had gained access to Capital One's sensitive data through a "misconfiguration" of a firewall on a web application. (A firewall monitors incoming and outgoing network traffic and blocks unauthorized access.) This allowed her to communicate with the server where Capital One was storing its data and customer files. Capital One stated it had immediately fixed the configuration vulnerability once it had been detected. Amazon said its customers fully control the applications they build and that it had found no evidence that its underlying cloud services had been compromised.

Thompson was able to access and steal this sensitive information only because Capital One had misconfigured its Amazon server. Thompson could then trick a system in the cloud to uncover the credentials she needed to access Capital One's customer records. Thompson's crime was considered an insider threat, since she had worked at Amazon years earlier. However, outsiders also try to search for and exploit this type of misconfiguration, and server misconfigurations are commonplace. Misconfigurations are also easily fixed, so many do not consider them a breach. Sometimes it's difficult to determine whether tinkering with misconfigurations represents a criminal activity or security research.

Thompson was able to tap into Amazon's metadata service, which has the credentials and other data required to manage servers in the cloud. Ms. Thompson ran a scan of the Internet to identify vulnerable computers that could provide access to a company's internal networks. She found a computer managing communications between Capital One's cloud and the public Internet that had been misconfigured, with weak security settings. Through that opening Thompson was able to request the credentials required to find and read Capital One data stored in the cloud from the metadata service. Once Thompson located the Capital One data, she was able to download them without triggering any alerts. Thompson also boasted online that she had used the same techniques to access large amounts of online data from other organizations.

Amazon has stated that none of its services, including the metadata service, were the cause of the break-in and that AWS offers monitoring tools for detecting this type of incident. It is unclear why none of these alerting tools triggered an alarm when Thompson was hacking into Capital One. Thompson began hacking Capital One on

March 12, 2019, but went undetected until an outside researcher tipped off Capital One 127 days later. According to C. J. Moses, deputy chief information security officer for AWS, Amazon restricts most staff members from accessing its broader internal infrastructure in order to protect against "witting or unwitting" data breaches.

Security professionals have known about misconfiguration problems and the ability to steal credentials from the metadata service since at least 2014. Amazon believes it is the customer's responsibility to solve them. Some customers have failed to do so. When security researcher Brenton Thomas conducted an Internet scan in February 2019, he found more than 800 Amazon accounts that allowed similar access to the metadata service. (Amazon's cloud computing service has over one million users.) But Thomas also found other cloud computing companies with misconfigured services as well, including Microsoft's Azure cloud.

Whatever the cloud service, the pool of talent capable of launching similar attacks is expanding. Given the nature of cloud services, any person who has worked on developing technology at any of the major cloud computing companies can learn how these systems work in practice.

Capital One had a reputation for strong cloud security. The bank had conducted extensive due diligence before deciding to move to cloud computing in 2015. However, before the giant data breach, Capital One employees had raised concerns internally about high turnover in the company's cybersecurity unit and tardiness in installing some software to help spot and defend against hacks. The cybersecurity unit is responsible for ensuring Capital One's firewalls are properly configured and for scanning the Internet for evidence of a data breach. In recent years there have been many changes among senior leaders and staffers. About a third of Capital One's cybersecurity employees left the company in 2018.

Sources: Robert McMillan, "How the Accused Capital One Hacker Stole Reams of Data from the Cloud," *Wall Street* Journal, August 4, 2019; Emily Flitter and Karen Weiser, "Capital One Data Breach Compromises Data of Over 100 Million," *New York Times*, July 29, 2019; James Randle and Catherine Stupp, "Capital One Breach Highlights Dangers of Insider Threats," *Wall Street Journal*, July 31, 2019. Peter Rudegeair, AnnaMaria Andriotis, and David Benoit, "Capital One Hack Hits the Reputation of a Tech-Savvy Bank," *Wall Street Journal*, July 31, 2019.

CASE STUDY QUESTIONS

1. What management, organization, and technology factors were responsible for the Capital One hack?
2. Was this an insider hack? Explain your answer.
3. What steps could have been taken to prevent the Capital One hack?
4. Should companies handling sensitive data use cloud computing services? Explain your answer.

Software Vulnerability

Software errors pose a constant threat to information systems, causing untold losses in productivity and sometimes endangering people who use or depend on systems. Growing complexity and size of software programs, coupled with demands for rapid delivery to markets, have contributed to an increase in software flaws or vulnerabilities.

A major problem with software is the presence of hidden **bugs** or program code defects. Studies have shown that it is virtually impossible to eliminate all bugs from large programs. The main source of bugs is the complexity of decision-making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

Zero defects cannot be achieved in larger programs. Complete testing simply is not possible. Fully testing programs that contain thousands of choices and millions of paths would require thousands of years. Even with rigorous testing,