In my blog I will be talking about a data breach that affected Bank of America. Data breaches are very common as they affect many organizations across the world. But a data breach happening to a bank is extremely crucial. Data breaches are when sensitive information gets exposed by unauthorized users. Nobody is immune to data breaches but establishing good data prevention tactics is key to keep an organization secure. Understanding technology and taking proper protocol can prevent your data from being breached. Now that you have a little background of my topic, I will discuss the cybersecurity attack. A data breach involving Infosys McCamish; a third-party financial software provider, exposed the address, date of birth, social security number, and account information of 57,028 Bank of America accounts. An unauthorized group called lock bit accessed the consumer's information through McCamish's system. When this happened bank of America gave customers affected a 2-year theft protection plan. This breach occurred on November 3rd, 2021, and Infosys McCamish notified bank of America about the breach on November 24, 2021. Bank of America then notified their customers about the breach on February 2nd, 2022. Affected customers were told to change passwords, reset passwords, enable two factor authentication, and monitor their accounts. This attack showed that third party services can increase the risk of cyber-attacks. This attack had nothing to do with bank of America, a third-party service compromised the information of the bank. So that shows there's a big gap in which attackers can get information. This is an example of a vulnerability that an attacker found between these two sources. Situations like this cause banks to get criticized for allowing third party systems to get certain access. Even though the exact method used to get access to this information wasn't public, it was likely a vulnerability exploited

between the two sources which allowed for something like this to occur. The removal of malware, enchanted security protocols, or any collaboration with the cybersecurity of bank America was unclear after the attack. The attacker of this data breach may have used many methods to gain access to the system. These methods can include exploiting vulnerabilities on the network, using zero-day vulnerabilities, ransomware, data dumping, and phishing attacks. A lot of cyber security attacks begin with phishing attacks. Attackers will send employees emails tricking them into giving out sensitive information. Cyber criminals can send emails looking like the Bank of America to request certain private information. Many cyber-attacks also exploit vulnerabilities in the network, once they gain proper access to credentials, they can access sensitive information. Even though banks are supposed to have complex networks, some institutions may have outdated software or improper cloud services. Cyber attackers can also rely on zero-day vulnerabilities to capture flaws in the system. Banks may have hardware that needs to be patched, in which attackers can exploit this vulnerability to bypass certain authentication to access information. Once attackers get access to sensitive information they can demand a ransom. Attackers can also release the sensitive information online to the public or sell it on illegal websites like the dark web. Sensitive information involving the bank is very crucial as attackers can release financial information which puts the consumers and bank at risk. This is how a lot of hackers extort bank institutions. There are multiple technologies and protocols that can be exploited during a data breach. Most attackers rely on weak security protocols, certain applications vulnerabilities, and network protocols. Banks that offer online banking are usually targeted the most when it comes to data breaches. There are certain web

features that expose certain vulnerabilities like SQL injection, cross site scripting, and remote code execution. Encryption is the main way organizations protect sensitive information, but attackers can still bypass it if the encryption is weak. If the encryption is too weak, attackers can use man in the middle attacks to gain access to certain credentials. Network protocols like remote desktop protocol and server message block can be used to gain access to certain bank information that isn't authorized. Data breaches that happen to banks have a major impact on society, it can make customers not trust the bank, put individuals at risk for identity theft and financial fraud, increased money investments in cybersecurity, and legal consequences. When a bank experiences a data breach consumers of this bank may feel uneasy about banking with them. Financial information being exposed is extremely crucial, as this type of information should be kept confidential. This may cause people to leave their bank as they are less likely to feel secure. When consumers' financial information gets stolen it puts them at risk for fraud and identity theft. Their information is now left open to the public in which their information can be sold or used. Banks can also face lawsuits or extreme fines by consumers who feel like their information wasn't secured properly, which can ruin the bank's reputation. When banks experience data breaches, they usually invest a lot of money in cybersecurity to keep consumers information safe. They developed good data breach prevention policies, better encryption, and higher cyber defense. Data breaches like this have major impacts on banks. It explains all the possible vulnerabilities attackers can use to gain certain information. With the rise of cybercrime institutions like the bank need to establish a system in which information can be kept more secure. To prevent any legal trouble with the law or face reputational

damage to their organization. For consumers who use banks it is essential that you monitor your accounts and report any suspicious activity. The best way to keep a good cybersecurity is to keep a strong password and enable two factor authentication. Understanding how technology works and how to address certain vulnerabilities within a system is essential for organizations like banks to know. Understanding this will allow them to defend against certain attacks they might face, which can keep their business safe and secure.

Bank of America Data Breach: What & How It Happened? | Twingate." *Twingate.com*, 2024, www.twingate.com/blog/tips/Bank%20of%20America-data-breach.

Maurer, Tim, and Arthur Nelson. "The Global Cyber Threat to Financial Systems." *International Monetary Fund*, Mar. 2021, www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.