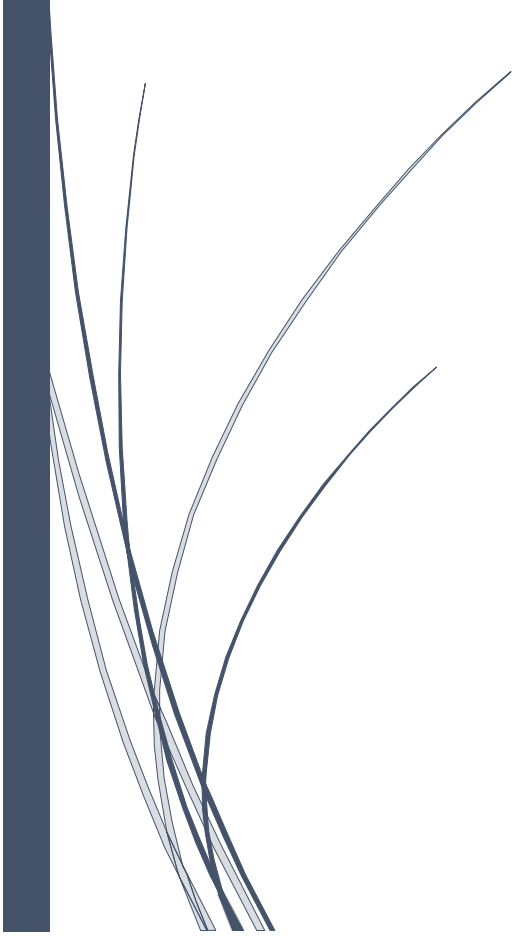
CYBER SECURITY
ESSENTIALS
REVIEW MATERIAL



Aan Systems, Inc

Monthly Review Material

Some of the Biggest Data Breaches of the 21st Century

Yahoo

Date: 2013-14
Impact: 3 billion user accounts
Details: In September 2016, the once dominant Internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by "a state-sponsored actor," in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm.

A couple of months later, in December, it buried that earlier record with the disclosure that a breach in 2013, by a different group of hackers had compromised 1 billion accounts. Besides names, dates of birth, email addresses and passwords that were not as well protected as those involved in 2014, security questions and answers were also compromised. In October of 2017, Yahoo revised that estimate, saying that, in fact, all 3 billion user accounts had been compromised.

The breaches knocked an estimated $350 million off Yahoo's sale price. Verizon eventually paid $4.48 billion for Yahoo's core Internet business. The agreement called for the two companies to share regulatory and legal liabilities from the breaches. The sale did not include a reported investment in Alibaba Group Holding of $41.3 billion and an ownership interest in Yahoo Japan of $9.3 billion.

eBay

Date: May 2014
Impact: 145 million users compromised
Details: The online auction giant reported a cyberattack in May 2014 that it said exposed names, addresses, dates of birth and encrypted passwords of all of its 145 million users. The company said hackers got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database.

It asked its customers to change their passwords, but said financial information, such as credit card numbers, was stored separately and was not compromised. The company was criticized at the time for a lack of communication informing its users and poor implementation of the password-renewal process.

CEO John Donahue said the breach resulted in a decline in user activity, but had little impact on the bottom line – its Q2 revenue was up 13 percent and earnings up 6 percent, in line with analyst expectations.

Heartland Payment Systems

Date: March 2008
Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's

data systems.
Details: At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175,000 merchants – most small- to mid-sized retailers. It wasn't discovered until January 2009, when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed.

Among the consequences were that Heartland was deemed out of compliance with the Payment Card Industry Data Security Standard (PCI DSS) and was not allowed to process the payments of major credit card providers until May 2009. The company also paid out an estimated $145 million in compensation for fraudulent payments.

A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban-American, was alleged to have masterminded the international operation that stole the credit and debit cards. In March 2010 he was sentenced to 20 years in federal prison. The vulnerability to SQL injection was well understood and security analysts had warned retailers about it for several years. Yet, the continuing vulnerability of many Web-facing applications made SQL injection the most common form of attack against Web sites at the time.

Uber

Date: Late 2016
Impact: Personal information of 57 million Uber users and 600,000 drivers exposed.
Details: The scope of the Uber breach alone warrants its inclusion on this list, and it's not the worst part of the hack. The way Uber handled the breach once discovered is one big hot mess, and it's a lesson for other companies on what not to do.

The company learned in late 2016 that two hackers were able to get names, email addresses, and mobile phone numbers of 57 users of the Uber app. They also got the driver license numbers of 600,000 Uber drivers. As far as we know, no other data such as credit card or Social Security numbers were stolen. The hackers were able to access Uber's GitHub account, where they found username and password credentials to Uber's AWS account. Those credentials should never have been on GitHub.

Here's the really bad part: It wasn't until about a year later that Uber made the breach public. What's worse, they paid the hackers $100,000 to destroy the data with no way to verify that they did, claiming it was a "bug bounty" fee. Uber fired its CSO because of the breach, effectively placing the blame on him.

The breach is believed to have cost Uber dearly in both reputation and money. At the time that the breach was announced, the company was in negotiations to sell a stake to Softbank. Initially, Uber's valuation was $68 billion. By the time the deal closed in December, its valuation dropped to $48 billion. Not all of the drop is attributable to the breach, but analysts see it being a significant factor.

JP Morgan Chase

Date: July 2014
Impact: 76 million households and 7 million small businesses
Details: The largest bank in the nation was the victim of a hack during the summer of 2014 that compromised the data of more than half of all US households – 76 million – plus 7 million small businesses. The data included contact information – names, addresses, phone numbers and email

addresses – as well as internal information about the users, according to a filing with the Securities and Exchange Commission.

The bank said no customer money had been stolen and that there was “no evidence that account information for such affected customers – account numbers, passwords, user IDs, dates of birth or Social Security numbers – was compromised during this attack."

Still, the hackers were reportedly able to gain “root" privileges on more than 90 of the bank’s servers, which meant they could take actions including transferring funds and closing accounts. According to the SANS Institute, JP Morgan spends $250 million on security every year.

In November 2015, federal authorities indicted four men, charging them with the JP Morgan hack plus other financial institutions. Gery Shalon, Joshua Samuel Aaron and Ziv Orenstein faced 23 counts, including unauthorized access of computers, identity theft, securities and wire fraud and money laundering that netted them an estimated $100 million. A fourth hacker who helped them breach the networks was not identified.

Shalon and Orenstein, both Israelis, pleaded not guilty in June 2016. Aaron was arrested at JFK Airport in New York last December.