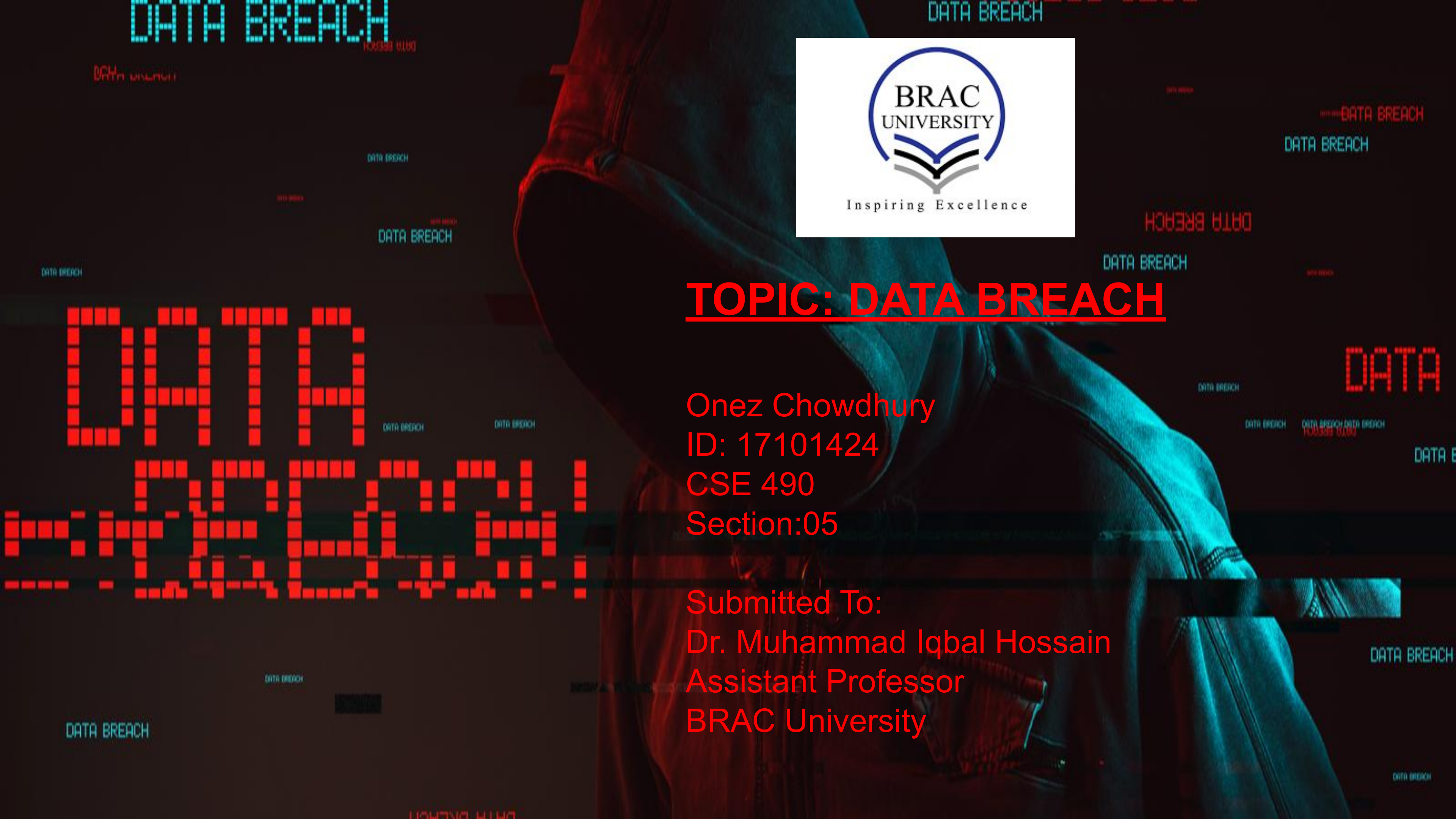


BRAC UNIVERSITY

Inspiring Excellence

TOPIC: DATA BREACH

Onez Chowdhury
ID: 17101424
CSE 490
Section:05

Submitted To:
Dr. Muhammad Iqbal Hossain
Assistant Professor
BRAC University

Data Breach

- What is Data breach ?

  A data breach is the intentional or unintentional release of secure/private/confidential information to an untrusted environment.

  - Device theft or loss
  - Document errors
  - Weak and stolen credentials
  - Internet spyware
  - Vulnerable systems and applications

BACKGROUND

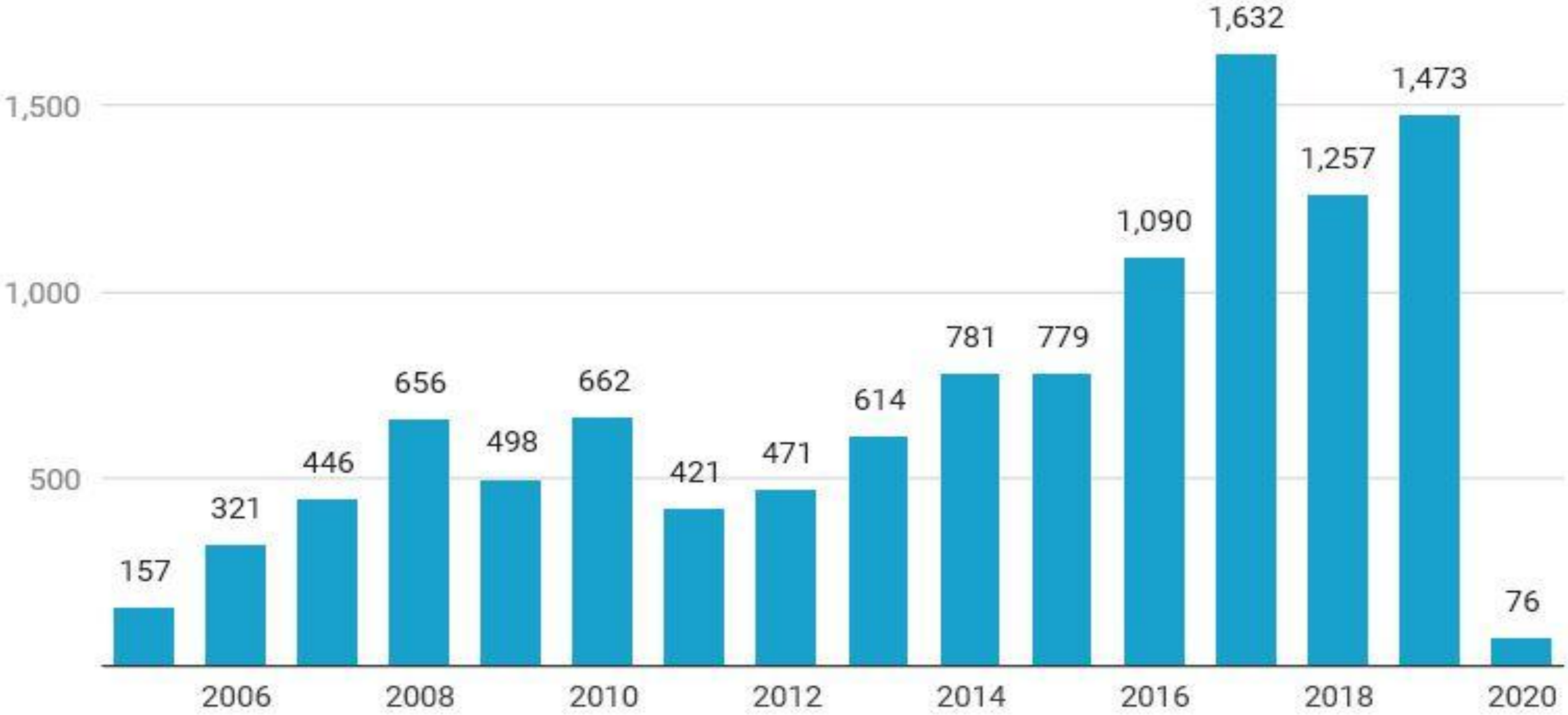
- ***Data Breaches*** increased in frequency in the 1980s, and in the 1990s and early 2000s, public awareness of the potential for **data breaches began** to rise.

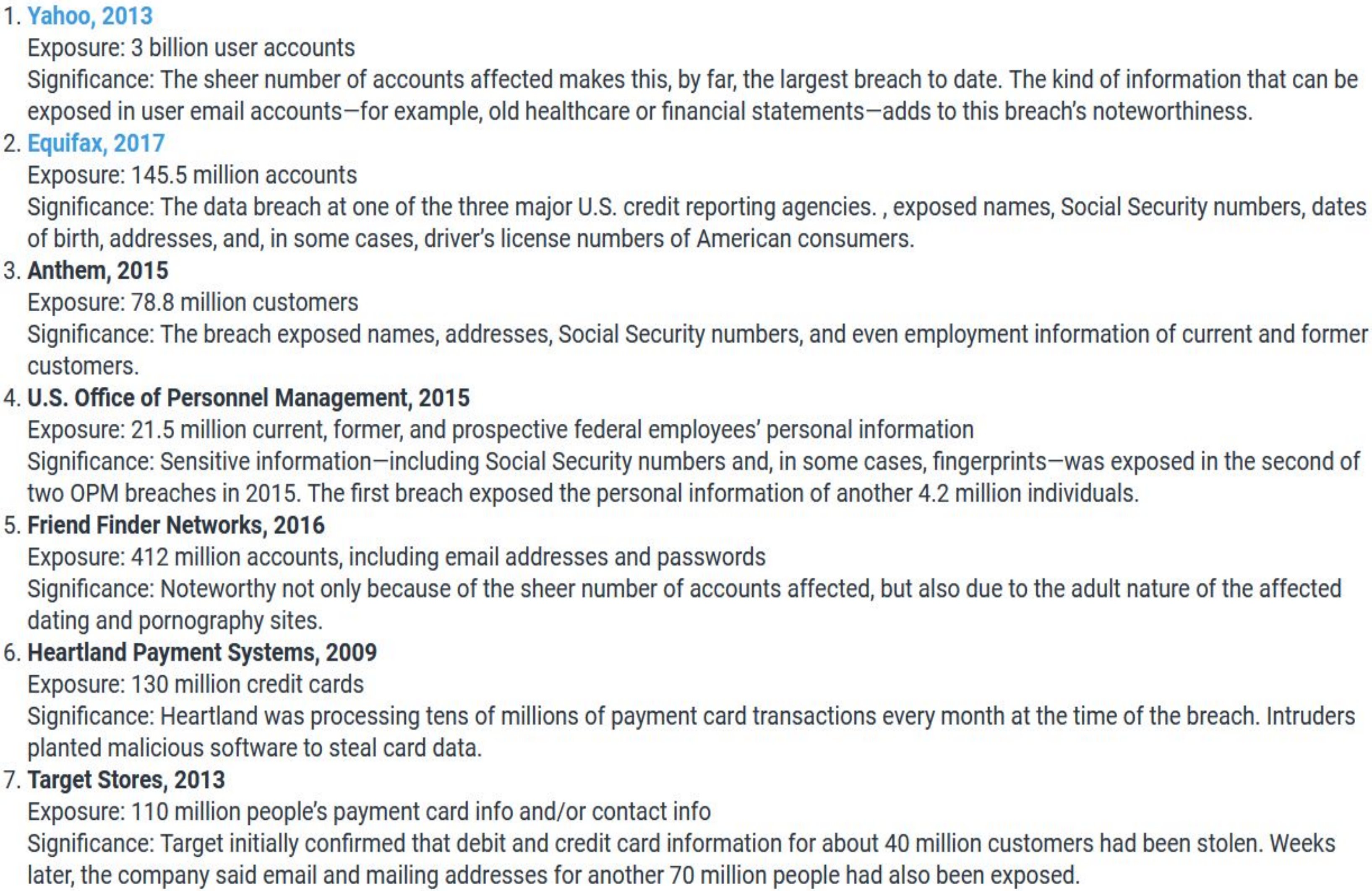
- 2005 is the year of the first data breach to compromise more than 1 million records.

- Most of the largest breaches have happened more recently than 2005.

Total number of breaches (2005–2020, to date)

Number of data breaches affecting US consumers.





1. Yahoo, 2013
   Exposure: 3 billion user accounts
   Significance: The sheer number of accounts affected makes this, by far, the largest breach to date. The kind of information that can be exposed in user email accounts—for example, old healthcare or financial statements—adds to this breach's noteworthiness.
2. Equifax, 2017
   Exposure: 145.5 million accounts
   Significance: The data breach at one of the three major U.S. credit reporting agencies. , exposed names, Social Security numbers, dates of birth, addresses, and, in some cases, driver's license numbers of American consumers.
3. **Anthem, 2015**
   Exposure: 78.8 million customers
   Significance: The breach exposed names, addresses, Social Security numbers, and even employment information of current and former customers.
4. **U.S. Office of Personnel Management, 2015**
   Exposure: 21.5 million current, former, and prospective federal employees' personal information
   Significance: Sensitive information—including Social Security numbers and, in some cases, fingerprints—was exposed in the second of two OPM breaches in 2015. The first breach exposed the personal information of another 4.2 million individuals.
5. **Friend Finder Networks, 2016**
   Exposure: 412 million accounts, including email addresses and passwords
   Significance: Noteworthy not only because of the sheer number of accounts affected, but also due to the adult nature of the affected dating and pornography sites.
6. **Heartland Payment Systems, 2009**
   Exposure: 130 million credit cards
   Significance: Heartland was processing tens of millions of payment card transactions every month at the time of the breach. Intruders planted malicious software to steal card data.
7. **Target Stores, 2013**
   Exposure: 110 million people's payment card info and/or contact info
   Significance: Target initially confirmed that debit and credit card information for about 40 million customers had been stolen. Weeks later, the company said email and mailing addresses for another 70 million people had also been exposed.

CAUSES OF DATA BREACH

1. Weak Passwords
2. Back Doors
3. Malware
4. Insider Threats
5. Physical Attack

DATA BREACH SECURITY STRATEGY

1. Reconnaissance
2. Email or malware attack
3. Prevent to use same password
4. Data stolen case
5. Use employee credentials

What should a company do after a data breach?

1. **Identify the Source and Extent of the Breach**
2. **Alert Your Breach Task Force and Address the Breach ASAP**
3. **Test Your Security Fix**
4. **Inform the Authorities and ALL Affected Customers**
5. **Prepare for Post-Breach Cleanup and Damage Control**

CONCLUSION

We discuss how data breaches affect the business and how it impact on the people. Also, studied how to prevent data breaches and popular attack and their controls. From this presentation, you will be able to know what is data breach, how it affect us and how to stop it.

REFERENCES

https://www.slideshare.net/burhanAhmed14/data-breach-129218661

https://www.lifelock.com/learn-data-breaches-history-of-data-breaches.html

https://www.whoa.com/5-steps-to-take-after-a-small-business-data-breach/