

IMUN<sup>22</sup>



UNCSTD

The Global issue of regulating cyber security procedures and forbidding data breaches

President:  
Hala Al Hassan

Chair(s):  
Sanad Zumut  
Maya Layous

## **Introduction**

Companies such as Facebook, Yahoo, Instagram, Uber, Tiktok and many more have been accused of gathering and retaining personal data on its clients. This is dangerous on numerous levels since these companies have access to private or sensitive information, such as a customer's address, occupation, or payment information. The objective is to collect and store as much data about customers as possible to aid businesses in developing better targeted advertisements and content, as well as improving their products and services. While this gives companies a competitive advantage, it also comes with a variety of risks. that include, Potential lawsuits from customers whose information has been exposed, Ransomware demands from attackers, Recovery costs such as restoring or patching systems that have been breached and even reputational damage and loss of customers.

## **General Information:**

In 2012, The Obama administration announced a \$200 million commitment to the Big Data Research and Development Initiative, citing the need to improve the ability to extract valuable insights from data, accelerate STEM (science, technology, engineering, and mathematics) growth, improve national security, and transform learning. Since then, the abbreviation has been shortened to STEAM, with the arts added as the "A". The best job of the twenty-first century, according to Harvard Business Review, is data scientist. Demand for data scientists surged as more businesses realized the need of sorting and gaining insights from unstructured data.

Later on in 2013, the global market reached 10 billion. In the year 2014 In the United States, mobile devices now outnumber desktop PCs for the first time. Two years later, in 2016, the rest of the globe followed suit.

According to IBM, 90% of the world's data was created in the last two years, and 2.5 quintillion bytes of data is created per day (that's 18 zeroes). According to Allied Market Research, the big data and business analytics market was valued at \$193.14 billion in 2019 and is predicted to rise at a CAGR of 10.9 percent to \$420.98 billion by 2027. In critical sectors, edge computing is expected to revolutionize the way data is maintained and processed. Edge computing, which refers to processing done near the source of data collection rather than in the cloud or a centralized data center, is the next frontier for big data.

China:

On July 4th, 2022, unknown hackers called "Chinadan" claimed to have breached and stolen personal data of 1 billion Chinese citizens from the Shanghai police database a year after the Personal Information Protection Law went into force in the country, requiring strict security measures from business and governmental organizations that handle personal information. The measure was approved as a result of Chinese

officials' demands that the parent businesses of more than 40 applications alter their business practices for breaking data transfer laws, according to Reuters.

Accordingly, the person or hacking group released a sample that contained 750,000 records. After that, the hacker or hacking group offered to sell more than 23 terabytes of stolen data from the database, that included names, addresses, medical records, birthplaces, national IDs, phone numbers and even private criminal case information from thefts to fights to domestic abuse, the leak included events that occurred between the late 1990s and 2019. Both the reported occurrences and the personal data were in different folders. The alleged hackers said that there were several billion police reports. The asking price of all the records was 10 bitcoin or even could accept \$200,000 cash.

People who have had their private information hacked online run the danger of experiencing physical damages including assault, harassment, and fraud. Numerous customers also complained of receiving "strange international phone calls," which they believed to be connected to the breach, according to Quartz.

Weibo Corp, states in 2020 that hackers had allegedly obtained account information for more than 538 million users, but those passwords and other critical information had not been disclosed. Additionally, a rights organization claims that this year, tens of thousands of allegedly breached data from China's remote Xinjiang province provide new proof of the mistreatment of primarily Muslim ethnic Uyghurs.

The most recent reported instance once again highlighted Beijing's difficulties as it continues to tighten its control over sensitive internet material while gathering data on hundreds of millions of individuals. Personal information disclosure is punishable by jail time in China.

It's unknown how the suspected cyberattackers in this month's incident got access to the systems belonging to the Shanghai police. Online among cybersecurity professionals, there was a prevailing view that the compromise included a third-party cloud infrastructure partner. Among the major foreign cloud services in the nation are Tencent Holdings Ltd., Huawei Technologies Co., and Alibaba Group Holding Ltd.

Data breaches have substantially expanded on a global scale. 308,000 databases, including more than 90,000 housed in the United States and more than 50,000 in China, were found to be accessible to the public web in 2021. However, the majority of these disclosures. This involved businesses or private organizations that kept records of their clients' or employees' personal information.

North Korea:

The FBI and private investigators have seized about \$30 million worth of cryptocurrency stolen from a video game company. US officials worry the money will be used to fund North Korea's nuclear weapons programs. The FBI said earlier this

year, hackers have stolen more than \$600 million from cryptocurrency firms around north Korea. North Korean government-backed hackers have stolen billions of dollars by invading cryptocurrency exchanges, according to the U.N.

The North Korean hackers have laundered stolen bitcoin, as well as other accounts they use to move money that have been sanctioned by in effort to stop them from targeting cryptocurrencies. Those efforts have made it more difficult for the hackers to cash out the stolen and laundered money.

In June 2021, representatives of the Justice Department have taken around half of the \$4.4 million ransom payment to Russian-speaking hackers. Colonial Pipeline (company) supplies about 45% of the petroleum used on the East Coast. However, the laundering still represents a tiny fraction of the yearly billions of dollars generated by cybercrime.

Suspected North Korean hackers conducted an espionage operation between February and July to obtain data on energy companies in the US, Japan, and Canada. According to US officials and cybersecurity experts, North Korean computer spies are charged with gathering important intelligence for the country's leadership.

## **Definition of Key Terms**

### Breached data:

A data breach is a situation in which information is taken from a system without the owner's knowledge or consent. A data breach might happen to a small business or a major corporation. Credit card numbers, customer information, trade secrets, and information pertaining to national security are examples of sensitive, proprietary, or private information that may have been stolen.

### Data Base:

A database is a planned grouping of material that has been arranged and is often kept electronically in a computer system. A database management system often oversees a database (DBMS). The term "database system," which is sometimes abbreviated to "database," refers to the combination of the data, the DBMS, and the applications that are connected to it.

### Laundering of money:

when people think of money laundry, they usually think of “washing money”. however, this is a term used in the business world as it generally refers to financial transactions in which criminals attempt to disguise the sources or nature of their illegal activities and where they have passive income of huge sums of money.

### Cybercrime:

Cybercrimes are crimes that take place in the means of technology of online. Examples of cybercrime include, identity theft, credit card fraud, cyber extortion and many more.

### Cryptocurrency:

a digital currency or a non-fungible currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Many people invest in cryptocurrency as it increases over the years and can use it to pay for other things. Examples of different cryptocurrencies include Bitcoin, Dogecoin, Ethereum...

### **Major Parties involved:**

#### United states:

The United States can be considered as a major party involved in this topic as it is the Largest country involved in the storage of data. Moreover, the USA is reported to be the country that has the most companies. An example of this is when Obama administration announces a \$200 million commitment to the Development Initiative. Meaning that the USA is willing to fix this global issue as they detect the cyber-attacks.

#### Facebook:

Facebook continues to gather data even after you leave its website. Any website you visit may already record information on you, including your IP address, the adverts you've clicked on, the browser you're using, and how frequently you visit the site. Over 533 million Facebook users' personal data from 106 different countries was exposed, including over 32 million records for US users, 11 million for UK users, and 6 million for Indian users. It contains their contact information, Facebook IDs, complete names, addresses, dates of birth, biographies, and, in some cases, email addresses. This makes Facebook the one of the companies with the highest stolen data rates and a huge part of this global issue.

#### Pentagon:

the pentagon is One of the largest office buildings in the world, the Pentagon serves as the headquarters of the United States Department of Defense. A symbol of American military strength, this concrete and steel building is recognized around the world. The Pentagon are involved in stolen data as the Department of Defense (DOD) announced the Pentagon data breach, but details were scarce. A spokesperson for the Pentagon said travel records including personal information and credit card data for about 30,000 individuals were involved.

#### China:

China is one of the largest producers of cybercriminals in the world, according to the US and other countries, who they claim hack into networks on behalf of local authorities in pursuit of valuable data or intellectual property. However, domestic violations are seldom reported due to a lack of open reporting channels.

### **Timeline of Events:**

1663: John Graunt pioneers statistical data analysis.

1664: first collection of public health data by collecting death rates and variations.

1865: reviewing data and then exploited that data to generate actionable information,

1884: The punch card tabulating machine invented

1890: tabulating equipment was used to tabulate data.

1911: Computing-Tabulating-Recording Company were established (IBM)

1928: a method for storing data on tape was developed.

1943: the UK developed a theoretical computer.

2012: Obama administration announces a \$200 million commitment to the Development Initiative

2013: global market reached 10 billion.

2014: In the United States, mobile devices now outnumber desktop PCs for the first time.

2016: the rest of the globe follows suit.

2019: analytics market was valued at \$193.14 billion

### **Useful Resources:**

<https://www.trendmicro.com/vinfo/us/security/definition/data-breach>

<https://www.bloomberg.com/cybersecurity>

<https://www.washingtonpost.com/business/2022/07/06/china-hack-police/>

<https://blog.cyberproof.com/blog/which-countries-are-most-dangerous>

<https://www.bloomberg.com/news/articles/2021-12-09/chinese-hackers-targeted-southeast-asian-nations-report->

[says#:~:text=Malaysia%2C%20Indonesia%20and%20Vietnam%20were,Cambodia%20and%20Thailand%2C%20it%20said](https://www.bloomberg.com/news/articles/2021-12-09/chinese-hackers-targeted-southeast-asian-nations-report-says#:~:text=Malaysia%2C%20Indonesia%20and%20Vietnam%20were,Cambodia%20and%20Thailand%2C%20it%20said)

<https://economictimes.indiatimes.com/news/international/world-news/data-leak-reveals-members-of-chinas-communist-party-working-in-global-firms-consulates-report/articleshow/79721469.cms>  
<https://www.varonis.com/blog/the-world-in-data-breaches>

## **Contact Information**

Expert Chair on Topic: Maya Layyous - [Maya\\_layyous@abs.edu.jo](mailto:Maya_layyous@abs.edu.jo)

Co- Chair: Sanad Zoumot – [Sanad\\_zumot@abs.edu.jo](mailto:Sanad_zumot@abs.edu.jo)

President: Hala Ali-Hassan – [Hala\\_alihassan@abs.edu.jo](mailto:Hala_alihassan@abs.edu.jo)