Information Security

PREPARED BY: DR. REEMA PATEL

SECURITY WORLD WIDE

Security Breach

- **What is a Data Breach?**
- A data breach is any incident where confidential or sensitive information has been accessed without permission.
- Breaches are the result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within.

Top data breach statistics for 2024

	Organisation name	Sector	Location	Known number of records breached	Month
1	MOAB	Multiple	Multiple	>26,000,000,000	January
2	Discord (via Spy.pet)	IT services and software	USA	4,186,879,104	April
3	Far Eastern Research Center for Space Hydrometeorology (Planeta)	Public	Russia	2 PB	January
4	Baidu, Inc., Honor, Huawei, iFlytek, OPPO, Samsung Electronics, Tencent, Vivo and Xiaomi Technology	IT services and software	China	Up to 1,000,000,000	April
5	Indian mobile network consumer database (probably)	Telecoms	India	750,000,000	January
6	Zenlayer	Telecoms	USA	384,658,212	February
7	Unknown Brazilian organisation	Unknown	Brazil	>223,000,000	January
8	Telekom Malaysia	Telecoms	Malaysia	Almost 200,000,000	January
9	Pure Incubation Ventures	Professional services	USA	183,754,481	February
10	916 Google Firebase websites	Multiple	USA	124,605,664	March

35,900,145,035
KNOWN RECORDS BREACHED
MONTHLY AVERAGE: **8,975,036,259**

9,478
PUBLICLY DISCLOSED INCIDENTS
MONTHLY AVERAGE: **2,370**

- Worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025, emphasizing the need for enhanced cybersecurity measures (Statista).
- Cybercrime losses reported to the FBI's Internet Crime Complaint Center (IC3) increased 22% between 2022 and 2023 (Federal Bureau of Investigation).

Most breached sectors of 2024

BY KNOWN RECORDS BREACHED

IT services & software

5,401,989,001

SECOND PLACE

Public: 2,137,250,984

BY PUBLICLY DISCLOSED INCIDENTS

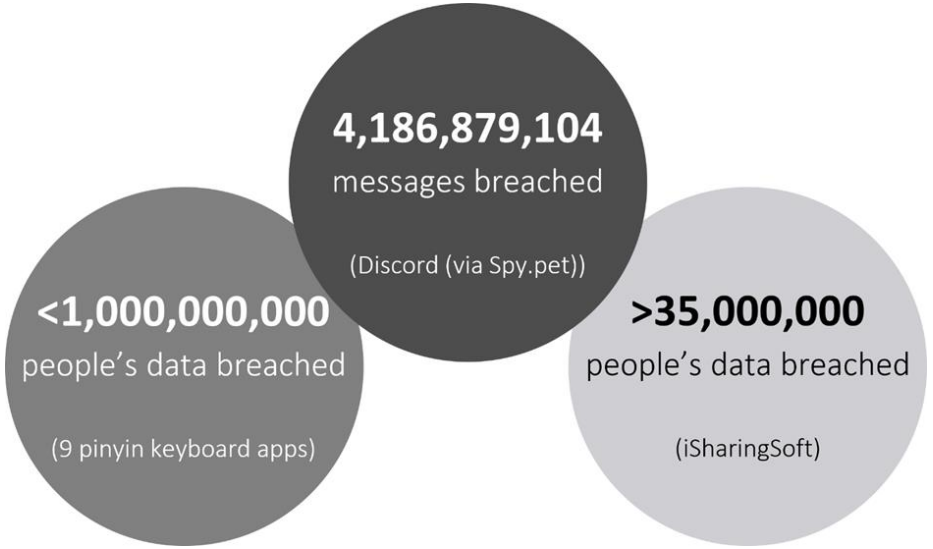
Healthcare

435 (17%)

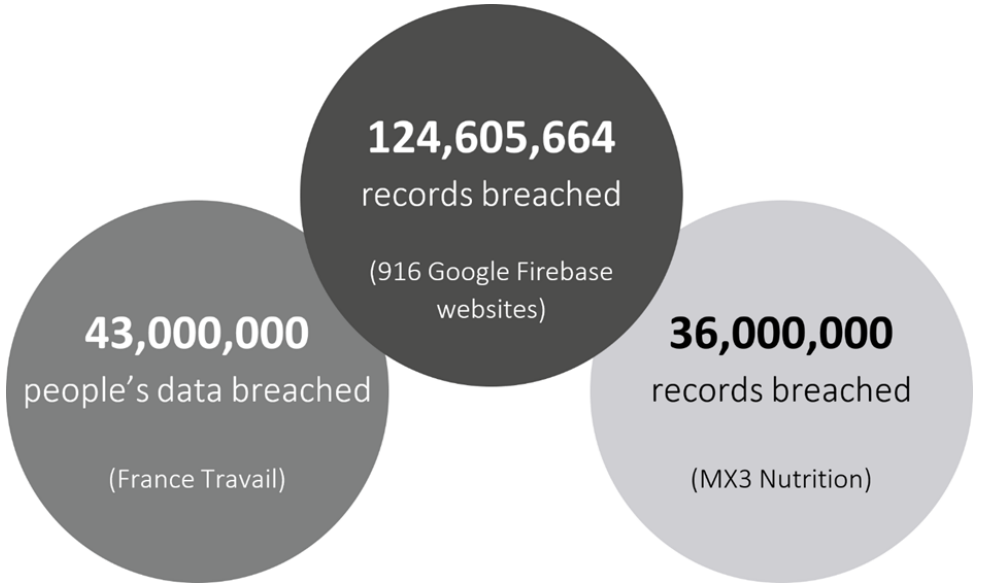
SECOND PLACE

Public: 419 (17%)

The top 3 biggest breaches in April 2024



The top 3 biggest breaches in March 2024



Top 5 most breached sectors (by number of incidents)

	Sector	Incidents	
1	Public	183	26%
2	Healthcare	98	14%
3	Manufacturing	67	10%
4	Retail	63	9%
5	Finance	55	8%

Top 5 most breached sectors (by number of records)

	Sector	Known number of records breached
1	Public	2,058,058,578
2	Telecoms	953,999,998
3	IT services and software	82,918,310
4	Finance	33,889,864
5	Education	31,038,133

Security Breach

- **July 2024**
- **July 15**
- **Disney Data Breach:** A hacking group going by the name “NullBulge” has managed to get its hands on reams of internal company Slack messages sent by employees of Disney. The messages – which were lifted from more than 10,000 channels and amount to around 1.2 TB of data – were allegedly obtained through a form of cookie hacking.

- **July 14**
- **AT&T Data Breach Update:** It has been revealed that telecommunications behemoth AT&T – which suffered a severe data breach this year impacting nearly all of its customers – paid $370,000 to a hacker to ensure that they deleted the customer information they’d extracted from the company’s system. The hackers were paid in Bitcoin back in May, Wired reports.

Security Breach

- **June 2024**
- **June 13**
- **Truist Bank Data Breach:** One of the largest banks in America – Truist Bank – reveals that it suffered a data breach back in October 2023 after employee information appeared for sale online. A hacking group known as Sp1d3r has claimed responsibility and is reportedly selling the dataset for around $1 million. Truist – which looks after more than $500 billion in assets and has 65,000 staff members on its payroll – said they notified "a small number of clients" at the time of the breach.
- **June 11**
- **Tile Data Breach:** Life360, the company behind the Tile tracker device, reveals that its **databases have been breached**, and that the company is being targeted for extortion. In a statement, the company shared that the affected data includes names, addresses, email addresses, phone numbers and Tile device identification numbers.
- **June 1**
- **Ticketmaster Data Breach:** Ticketmaster confirms a **rumored data breach** from earlier in the year that saw records for its customers, including name, address, phone number, email address, order history and partial payment information, being offered for sale by hackers. Over 560 million customers are expected to be impacted.

Security Breach

- **May 2024**
- **May 13**
- **Helsinki City Council Data Breach:** Local government systems in the Finnish capital Helsinki have suffered a data breach after a hack targeted at their education systems.
- Students and guardians may have had their personal information stolen from the system by a threat actor who managed to find a way in via a remote access server. The hack is known to have occurred at the beginning of the month, but that information was only made public by city officials this week.
- **May 10**
- **JPMorgan Chase Data Breach:** The Maine District Attorney's Office has been notified that almost half a million people banking with JPMorgan Chase could have had their personal information extracted from the company's systems thanks to a software flaw dating back to 2021.
- Luckily, at present, there seems to be no evidence of foul play or the data being misused in any manner. It could, however, have been accessed by authorized parties associated or working with the bank at the time.
- **May 9**
- **Dell Data Breach:** Dell emails customers to inform that that their data may have been compromised after an attack on its customer portal. According to Dell, while no financial information was accessed, customers home addresses and order information may have been compromised. Data purportedly from the breach is being offered for sale on hacker forums, suggesting details of 49 million customers have been obtained.
- **May 1**
- **Dropbox Data Breach:** Dropbox tells users that its **Dropbox Sign** service has been accessed by a threat actor, who was able to see data including email addresses, phone numbers, hashed passwords and multi factor authenticator details. Dropbox cloud customers are unaffected.

Security Breach Incidents

- Crypto.com Crypto Theft – January 2022
- The attack took place on January 17th and targeted nearly 500 people's cryptocurrency wallets.
- In this case, hackers stole approximately $18 million worth of Bitcoin and $15 million worth of Ethereum, plus other cryptocurrencies.
  - This was primarily possible thanks to the hackers' ability to bypass two-factor authentication and access users' wallets.
- Initially dismissing the attack as an 'incident,' Crypto.com later retracted its statement, confirming that money had been stolen and that affected users had been reimbursed.
- The company also announced that it had audited systems and improved the organization's security posture. Businesses must be aware of the risks associated with cryptocurrency theft.
- The best way to protect against this type of fraud is to ensure that all sensitive data is encrypted.

Security Breach Incidents

- Microsoft Data Breach – March 2022
- Microsoft was targeted by a hacking group called Lapsus$.
- he group posted a screenshot on Telegram indicating they had hacked Microsoft, and in the process, compromised Cortana, Bing, and several other products.
- The hackers retrieved some material from Microsoft, but by March 22nd Microsoft announced it had quickly stopped the hacking attempt and only one account was compromised.
- Microsoft also said that no customer data had been stolen.
- In this case, Microsoft benefitted from the publicity it received for its effective security response.
- The Lapsus$ group had previously targeted Nvidia, Samsung and plenty of other companies, so Microsoft's security team was ready.

Security Breach Incidents

- April 2021
  - Facebook had no plans to notify individuals whose information was exposed because the company claims it does not know who was affected.
  - Despite the patch in September 2019, 419 million records were leaked which contained user IDs and phone numbers.
  - In December 2019, a Ukrainian researcher discovered a database on the open Internet which included the personal information of more than 267 million Facebook users.

Security Breach Incidents

- Microsoft Exchange
- On March 2, 2021, security firm Volexity uncovered a Microsoft vulnerability that allows hackers to take advantage of an Exchange Server flaw.
- It appears the threat actors have been planting web shells that enable administrative access and the ability to steal data as far back as January. The victims were targeted through their self-hosted Outlook Web Access manager.
- Bloomberg reported that 120,000 systems had been infected and less than 10,000 remained unpatched as of March 22, 2021.

Security Breach Incidents

- In March, the University of California (UC) announced it was the victim of a ransomware attack that targeted vulnerabilities in Accellion's legacy File Transfer Appliance (FTA).

- The stolen data included the personal information of faculty and students including their email addresses to which messages were said stating, "Your personal data has been stolen and will be published."

Security Breach Incidents

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.
- The Colonial Pipeline company halted all pipeline operations to contain the attack.
- Overseen by the FBI, the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million) within several hours;
- upon receipt of the ransom, an IT tool was provided to the Colonial Pipeline Company by DarkSide to restore the system.
  - However, the tool had a very long processing time to help get the system back up in time.

Security Breach Incidents

- The Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9.
- It was the largest cyberattack on an oil infrastructure target in the history of the United States.
- The FBI and various media sources identified the criminal hacking group DarkSide as the responsible party.
- The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack.
- On June 7, the Department of Justice announced that it had recovered 63.7 of the bitcoins (approximately $2.3 million) from the ransom payment.

Security Breach Incidents

- **Zoom**
- **April 14, 2020:** The credentials of over 500,000 Zoom teleconferencing accounts were found for sale on the dark web and hacker forums for as little as $.02.
- Email addresses, passwords, personal meeting URLs, and host keys are said to be collected through a credential stuffing attack.

- **Microsoft**
- **January 22, 2020:** A customer support database holding over 280 million Microsoft customer records was left unprotected on the web.
- Microsoft's exposed database disclosed email addresses, IP addresses, and support case details. Microsoft says the database did not include any other personal information.

Data from: https://www.identityforce.com/blog/2020-data-breaches

Security Breaches

- **Toyota's Second Data Breach Affects Millions Of Drivers**
- Toyota revealed the issue on its official website on March 29, 2019, saying the breach potentially affected 3.1 million people.
- The company said it did not believe the hackers accessed private customer or employee data in that instance.

Security Breaches

- **Investigation Of Walmart Email Breach**
- The FBI is investigating allegations that employees from one of Walmart's technology suppliers was illegally monitoring the retailer's e-mail communication.
- The New York Times reports that in late 2015 through early 2016, Compucom employees assigned to Walmart's help desk were using their access to monitor specific e-mail accounts at the retailer and allegedly using that information to get an edge over competitors.

Security Breaches

- **Customs and Border Protection Contractor Perceptics – May 2019**
- In May, a surveillance contractor for US Customs and Border Protection suffered a breach, and hackers stole photos of travelers and license plates related to about 100,000 people.

- **Ransomware**
- Criminal groups continue to target businesses, health care providers, and, most visibly, local governments with these brash hacks, in which malware is used to encrypt a system's data and then demand a ransom to decrypt it—swindling victims of billions of dollars a year in the process.

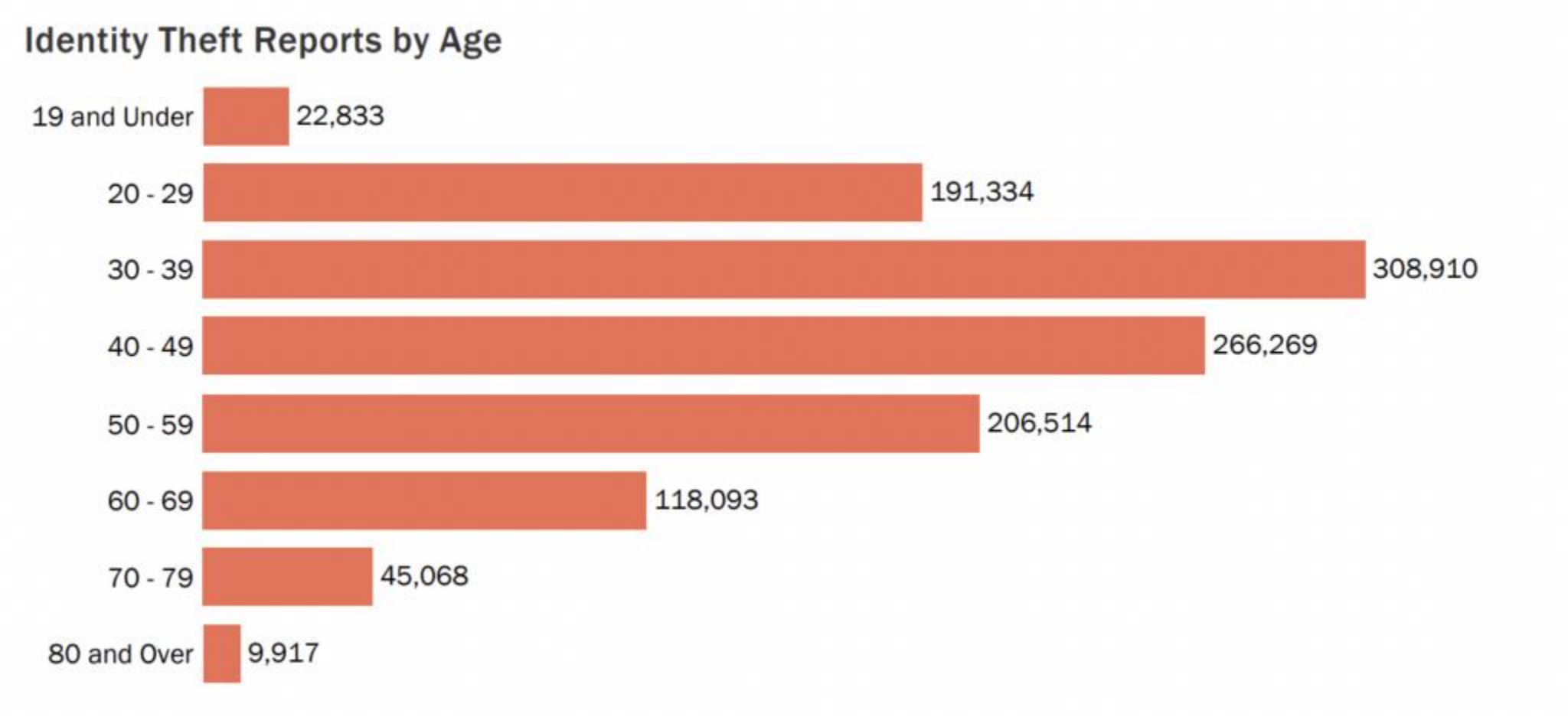
Security Breaches

- **American Medical Collection Agency breach**
- One of the most concerning corporate data breaches so far is that of the American Medical Collection Agency, a massive health-care-related debt collector.
- 12 million patients records exposed
- the compromised information included first and last names, dates of birth, phone numbers, addresses, dates of medical services, health care providers, and data on balances due

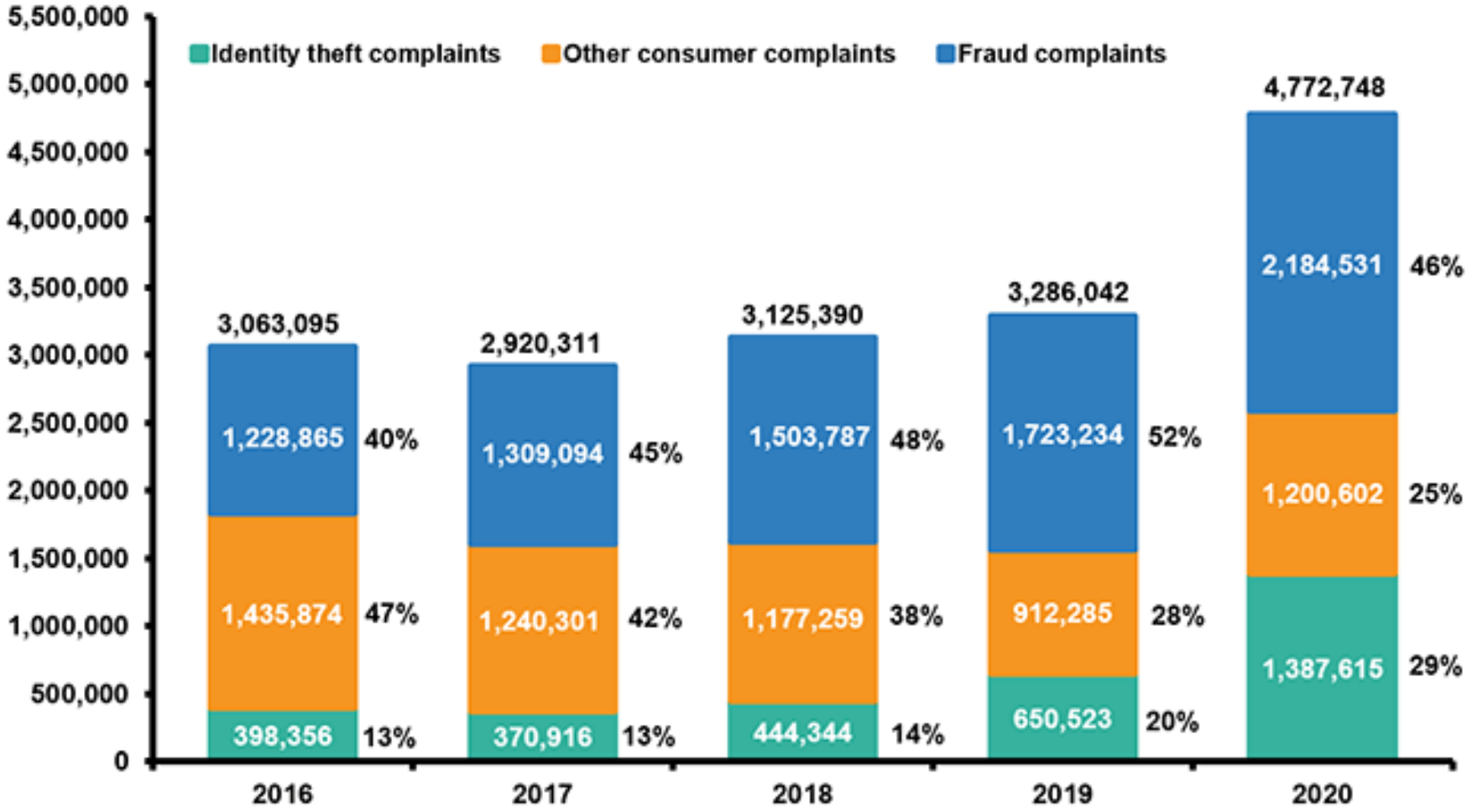
Security Breaches

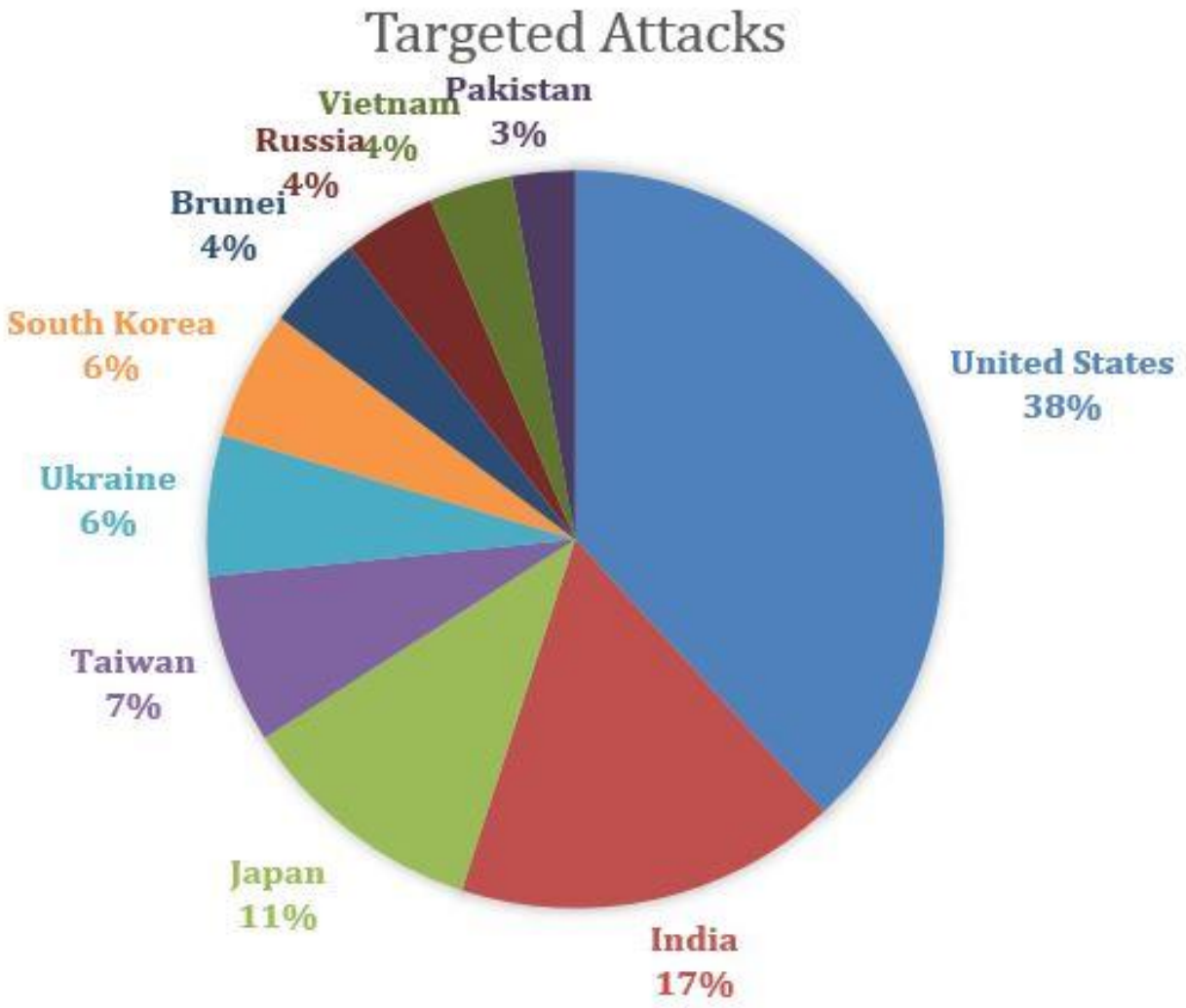
- **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**
- The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box.

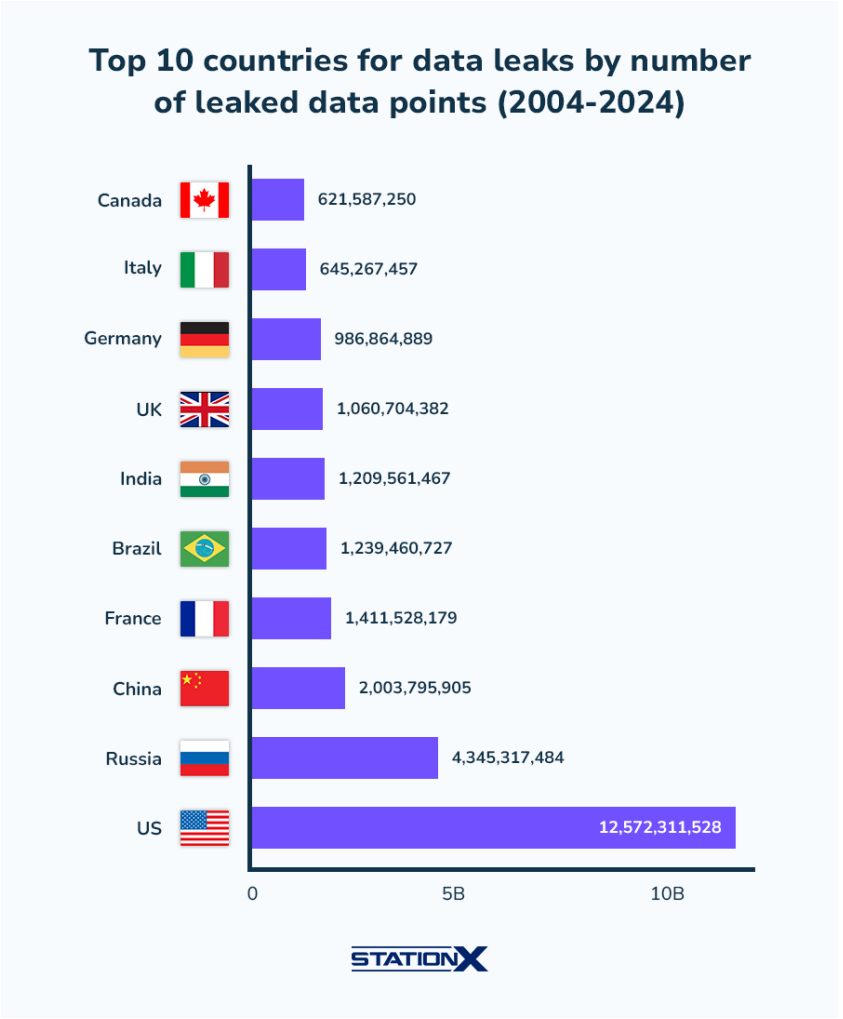
2024 Identity Theft Facts and Statistics



Publicly available numbers from Javelin Strategy & Research


Identity theft complaints
Other consumer complaints
Fraud complaints
5,500,000
5,000,000
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
3,063,095
1,228,865
40%
1,435,874
47%
398,356
13%
2,920,311
1,309,094
45%
1,240,301
42%
370,916
13%
3,125,390
1,503,787
48%
1,177,259
38%
444,344
14%
3,286,042
1,723,234
52%
912,285
28%
650,523
20%
4,772,748
2,184,531
46%
1,200,602
25%
1,387,615
29%
2016
2017
2018
2019
2020


Targeted Attacks
Vietnam
Pakistan
3%
Russia
4%
4%
Brunei
4%
South Korea
6%
United States
38%
Ukraine
6%
Taiwan
7%
Japan
11%
India
17%

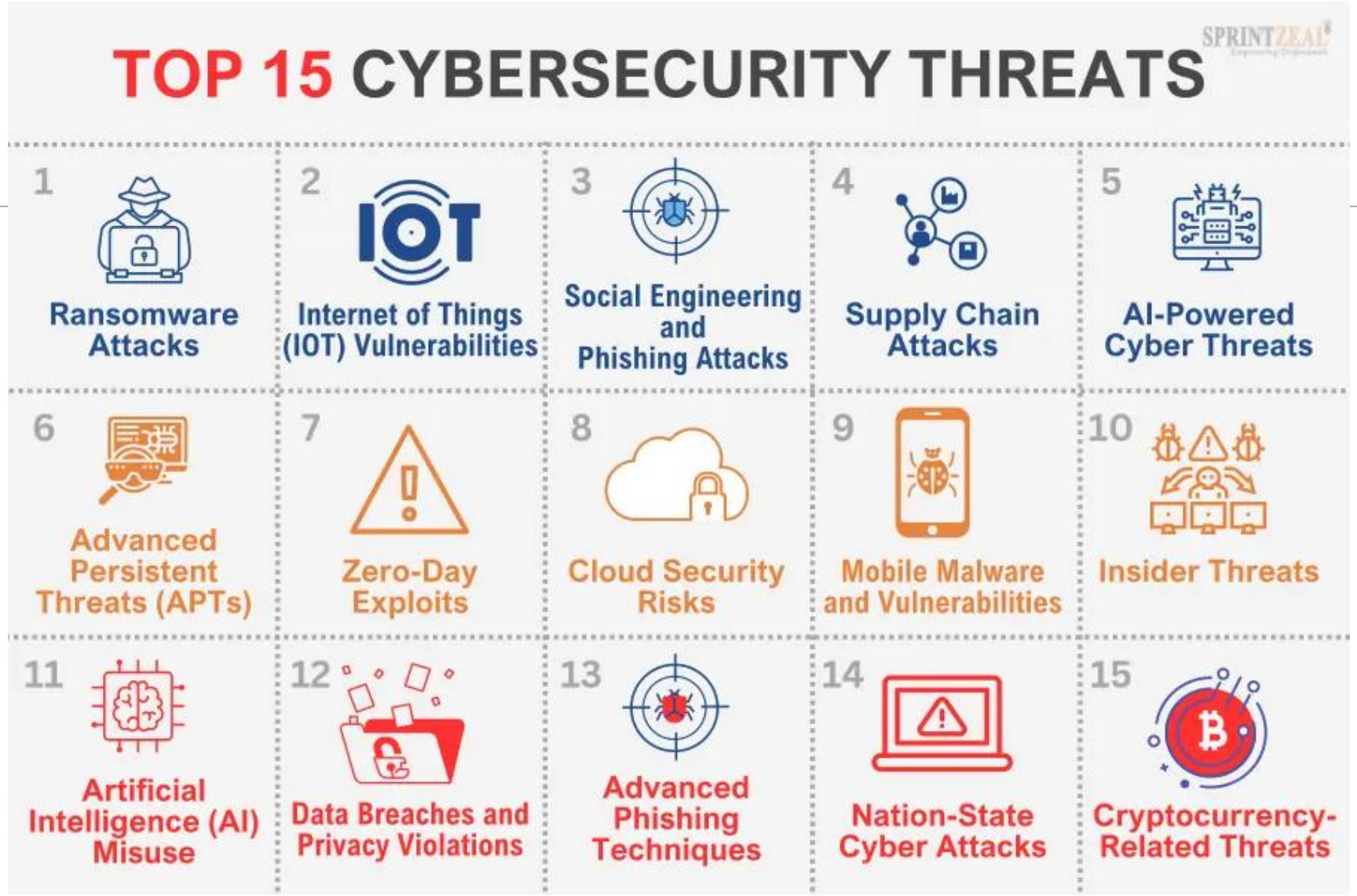

Top 10 countries for data leaks by number of leaked data points (2004-2024)
Canada
621,587,250
Italy
645,267,457
Germany
986,864,889
UK
1,060,704,382
India
1,209,561,467
Brazil
1,239,460,727
France
1,411,528,179
China
2,003,795,905
Russia
4,345,317,484
US
12,572,311,528
0
5B
10B
STATIONX

Largest disclosed company breaches or leaks

2009 – 2018 In (M)

Average cost of a data breach rises

- Cost of the average data breach to companies worldwide: $3.86 million (U.S. dollars)
- Cost of the average data breach to a U.S. company: $7.91 million (U.S. dollars)
- Average time it takes to identify a data breach: 196 days


TOP 15 CYBERSECURITY THREATS
SPRINTZEAL
1
Ransomware Attacks
2
IOT
Internet of Things (IOT) Vulnerabilities
3
Social Engineering and Phishing Attacks
4
Supply Chain Attacks
5
AI-Powered Cyber Threats
6
Advanced Persistent Threats (APTs)
7
Zero-Day Exploits
8
Cloud Security Risks
9
Mobile Malware and Vulnerabilities
10
Insider Threats
11
Artificial Intelligence (AI) Misuse
12
Data Breaches and Privacy Violations
13
Advanced Phishing Techniques
14
Nation-State Cyber Attacks
15
Cryptocurrency-Related Threats

Course Content

- **UNIT I**
- Introduction to Security, Security Basics – Confidentiality, Integrity, Availability; Introduction to types of attacks, Introduction to Security Threats: Viruses and Worms, Intruders, Insiders, Terrorists, Information warfare, Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection, Buffer Overflow, Brute Force.

Course Content

- **UNIT II:**
- Review of Number Theoretic Algorithms, Symmetric Encryption and Hash Function: Introduction to Symmetric encryption; Asymmetric encryption, Encryption algorithm / Cipher, Encryption and Decryption using: Caesar's cipher, play fair cipher, shift cipher, shift cipher, Vigenere cipher, one time pad (vermin cipher), hill cipher, Transposition techniques, Modern Block Ciphers, Symmetric Cryptographic Algorithms, Hashing function:SHA1

Course Content

- **UNIT III**
- Asymmetric encryption & Public Key Infrastructure: Diffie-Hellman, RSA, Digital Signatures, Public key infrastructures: basics, digital signatures, digital certificates, certificate authorities, registration authorities, Trust Models: Hierarchical, peer to peer.
- **Organizational Security:** Password selection, Piggybacking, Shoulder surfing, Dumpster diving, installing unauthorized software /hardware, Access by non-employees, Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers, Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.

Course Content

- **UNIT IV**
- Network Security: Firewalls: working, design principles, trusted systems, Kerberos, IP security: overview, architecture, IPSec configurations, IPSec security, Security topologies, Email security.
- Web Security: Intruders: Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, Intrusion detection systems, Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL); Transport Layer Security(TLS)

Reference Books

1. Principles Of Computer Security CompTIA Security And Beyond (Exam SY0-301), 3rd Edition, Conklin, Wm. Arthur Gregory White, Dwayne Williams, Mc Graw Hill
2. **Cryptography and Network Security Principles and Practices, Williams Stallings, Pearson Education, Third Edition**
3. **Cryptography and Network Security , B A Forouzen , TMH**
4. **Cryptography and Network Security Principal and Practices , Atul Kahathe, TMH**
5. Computer Security , Dieter Gollman , Wiley India Education, Second Edition