a₹tha

A NEWSLETTER OF THE FINANCE LAB

March 2021, Volume 6, Issue 4

INDIAN INSTITUTE OF MANAGEMENT CALCUTTA

INDIAN INSTITUTE OF MANAGEMENT CALCUTTA

Financial Research & Trading Laboratory

The Cost of Data Breaches

Yash Sharma

Yash Sharma is a Chartered accountant by profession, currently working with Swiggy. He cleared his CA in 2018 and is interested in the world of startups and ecommerce. Outside work, he likes badminton & swimming.

Introduction

Instead of starting with a cliché statement, I will start with a fact. In the year 2020, the estimated loss to the global economy due to data breaches is pegged at around $945 billion, or about 1% of global GDP. This is up about 80% from two years ago and in addition to about $145 billion spent on cybersecurity in 2020.[2]

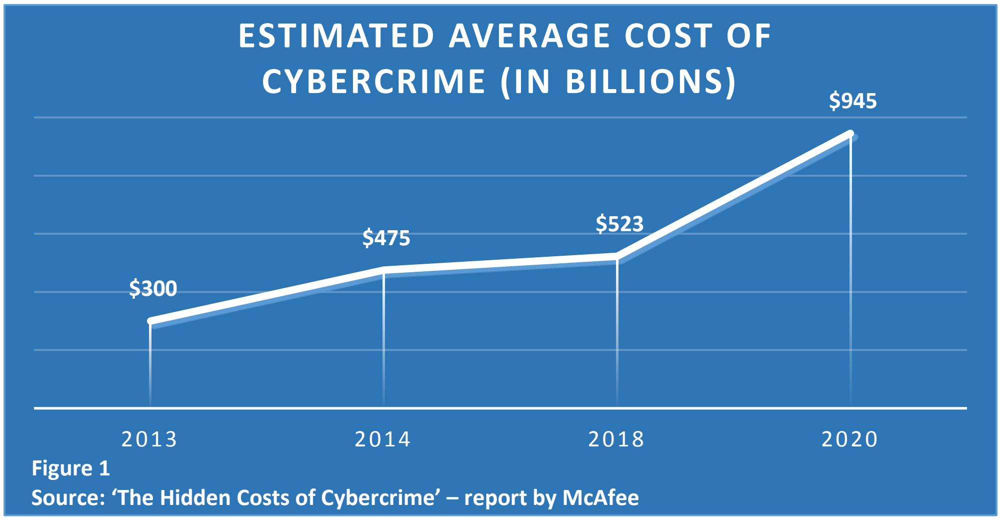


Figure 1
Source: 'The Hidden Costs of Cybercrime' – report by McAfee

In this article, we understand what data and sensitive data mean, what incentivizes data breaches, and what does it cost everyone, financially and otherwise. Besides, we look at some of the biggest data breaches in the past few years and understand what is changing to prevent them in the future.

Data, Personal Data, and Sensitive Data

To understand why breaches (both intentional and unintentional) happen and why it sounds so serious, we need to understand what data and its variants mean.

[2] 'The Hidden Costs of Cybercrime' – report by McAfee

In simplest of terms, any activity which takes place -- from the level of a little ant nest to a gigantic planetary-scale -- generates data. In that sense, data is simply bits of information. Even our existence gives rise to many data like age, gender, residence, and the list is practically endless. But not every data piece is economically attractive.

Personal data, on the other hand, means any detail through which one can identify, with some accuracy, a living person. However, every bit of personal information cannot be termed as personal data. For example, only by the name Yash Sharma you cannot identify me. There can be many others by the same name. If you however have the address and a phone number coupled with it, the name becomes a part of personal data.

And finally, the last piece of the puzzle, sensitive personal data. If any person's ethnic origin, political opinion, or similar detail can be identified by any information, it will be considered sensitive personal data. This data requires the highest level of scrutiny and security because it can bias judgment and opinion towards another person. To understand the importance of data privacy & security, imagining what could happen if someone with malicious intent or opportunistic mindset gets hold of your sensitive personal information.

What are Data Privacy and Data Security?

Access to sensitive data always yielded power. If someone knew any personal detail about you, he could have always used it for his gain or your loss. So, why the debates on the security of data now? Earlier, the data used to be collected and stored on paper and its summarization and use was a time-consuming process. As we entered the digital world, everything went paperless and you started getting notifications from shopping websites as soon as you googled any product.

In that context, a plethora of data can be summarized in minutes and can be turned into tangible profits with a specific area of focus. The sheer volume and speed of availability of data are what makes data privacy and security more important today.

Data privacy can be explained as policies and steps taken to ensure proper collection and usage of data. It is concerned with ensuring that the data is obtained with the user's consent and is accessible only to people and for the purpose consented by the owner of data.

Data security, on the other hand, is the method to ensure data privacy. These can include both physical controls, like locking the data servers in a cabin, as well as logical controls, like restricting access to limited authorized users.

Suppose an organization collected my name and age through an online form. The bottom of the form described how the data would be used and who could use the data, and the organization asked for my consent for the same.

This would be part of the data privacy policy. Once the data got stored on the organization's servers, the data was encrypted, the servers were put into a locked room and access to my data was protected by a password available to certain people only. This would be data security to ensure what the organization told me under the data privacy policy is upheld.

Data Breaches: What and Why

The collection and usage of data are taking the center stage while policy formulations of any function in almost all organizations. Hence, having robust data privacy and security policy becomes of paramount importance. Yet, as visible from Figure 2, only a small proportion of organizations have a plan to both prevent and respond to IT threats.

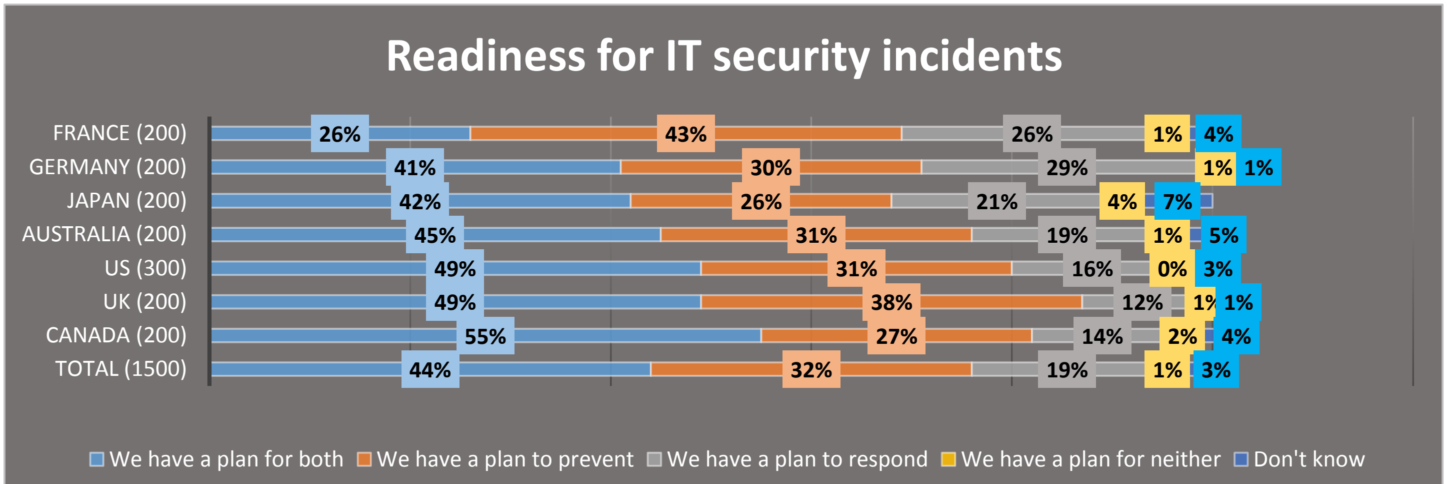


Figure 2
Source: 'The Hidden Costs of Cybercrime' - report by McAfee

In such a situation, there is a good chance of the occurrence of a data breach. Simply put, a data breach occurs when sensitive information is accessed by someone who was not authorized to have it. Such breach can even be unintentional. For example, at the beginning of 2018, the Defense Travel System (DTS) of the US Department of Defense (DOD) accidentally sent out an unencrypted mail with an attachment to a wrong distribution list. The mailer exposed personal details of about 21,500 U.S. marines, sailors & civilians; the details also included their bank account numbers, truncated Social Security numbers and emergency contact info.[3,4]

There is an even more significant threat of intentional data breach, referred to as 'hacking'. Traditionally, the people who wanted to hack into a piece of code had to be the people who had the ability and knowledge. And

[3] https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role

[4] https://www.marinecorpstimes.com/news/your-marine-corps/2018/02/28/major-data-breach-at-marine-forces-reserve-impacts-thousands/

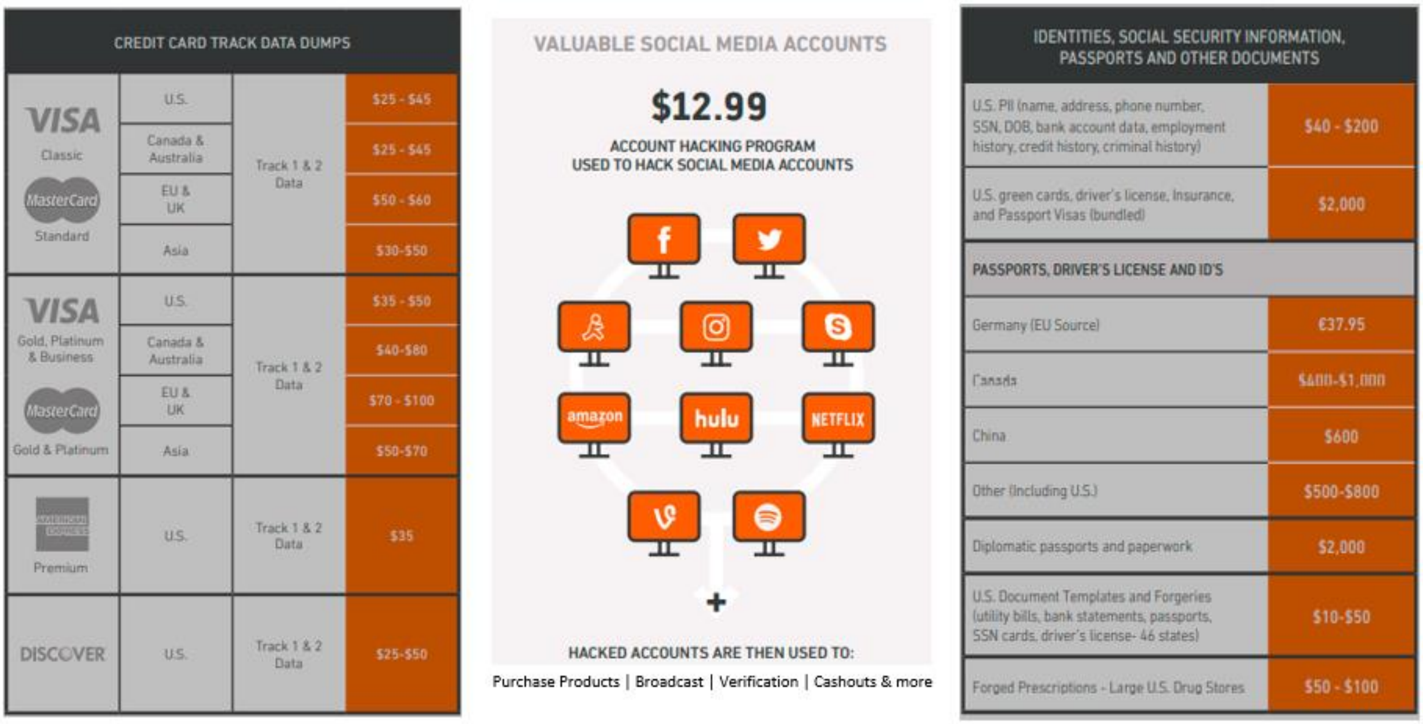
then there were problems of doing the research, arranging the infrastructure, and selling the spoils after a successful attack, which not every hacker wanted to do.

Enter outsourcing and e-marketplaces. Any common person, with no knowledge of coding but only an intent, can now outsource all the services: from research to infrastructure to the entire attack. Outsourcing provides convenience to both sellers and buyers. Some of the variants for services include:[5]

i. Research as a service, which covers finding vulnerabilities in a system and tools to exploit them
ii. Crimeware as a service, where code development and malware are provided
iii. Cybercrime infrastructure as a service, which covers spamming services and botnets, and lastly
iv. Hacking as a service, which covers cracking passwords and launching distributed denial-of-service (DDoS) attacks.

All the foregoing arguments beg the question, why do data breaches, at least intentional ones, take place? The answer: it is a profitable undertaking. To understand this, let us briefly look at the value of various data pieces in the market and the cost to acquire them.

When it comes to the dark web, everything is a fair game. You can find bulk Instagram account, credit card details, bank account details, citizenship & identity details and even the tools used to obtain all the above. From a value perspective, Figure 3 depicts their price in the black market.Figure 4 outlines the costs to organize different



CREDIT CARD TRACK DATA DUMPS			
VISA Classic MasterCard Standard	U.S.	Track 1 & 2 Data	$25 - $45
	Canada & Australia		$25 - $45
	EU & UK		$50 - $60
	Asia		$30-$50
VISA Gold, Platinum & Business MasterCard Gold & Platinum	U.S.	Track 1 & 2 Data	$35 - $50
	Canada & Australia		$40-$80
	EU & UK		$70 - $100
	Asia		$50-$70
AMERICAN EXPRESS Premium	U.S.	Track 1 & 2 Data	$35
DISCOVER	U.S.	Track 1 & 2 Data	$25-$50

VALUABLE SOCIAL MEDIA ACCOUNTS

$12.99

ACCOUNT HACKING PROGRAM
USED TO HACK SOCIAL MEDIA ACCOUNTS

HACKED ACCOUNTS ARE THEN USED TO:

Purchase Products | Broadcast | Verification | Cashouts & more

IDENTITIES, SOCIAL SECURITY INFORMATION, PASSPORTS AND OTHER DOCUMENTS	
U.S. PII (name, address, phone number, SSN, DOB, bank account data, employment history, credit history, criminal history)	$40 - $200
U.S. green cards, driver's license, Insurance, and Passport Visas (bundled)	$2,000
PASSPORTS, DRIVER'S LICENSE AND ID'S	
Germany (EU Source)	€37.95
Canada	$400-$1,000
China	$600
Other (Including U.S.)	$500-$800
Diplomatic passports and paperwork	$2,000
U.S. Document Templates and Forgeries (utility bills, bank statements, passports, SSN cards, driver's license- 46 states)	$10-$50
Forged Prescriptions - Large U.S. Drug Stores	$50 - $100

Figure 3
Source: 'THE BLACK MARKET REPORT - A look inside the Dark Web' - report by Armor

[5] 'Cybercrime exposed: Cybercrime-as-a-service' – report by McAfee

forms of data breaches. A banking trojan, for example, costs an average of $3,500. The number of total accounts affected globally (only a limited set of Kaspersky protection users) was around 900,000.[6] Assume a trojan campaign sends spam to only 500 US accounts. Even if we consider a 70% click rate of spam and assuming the hacker can get bank info of about 50% of the people who clicked the spam mail, it makes 175 accounts.[7] The median savings bank balance in America $4,500.[8] So, on average, the campaign can yield about $750,000.

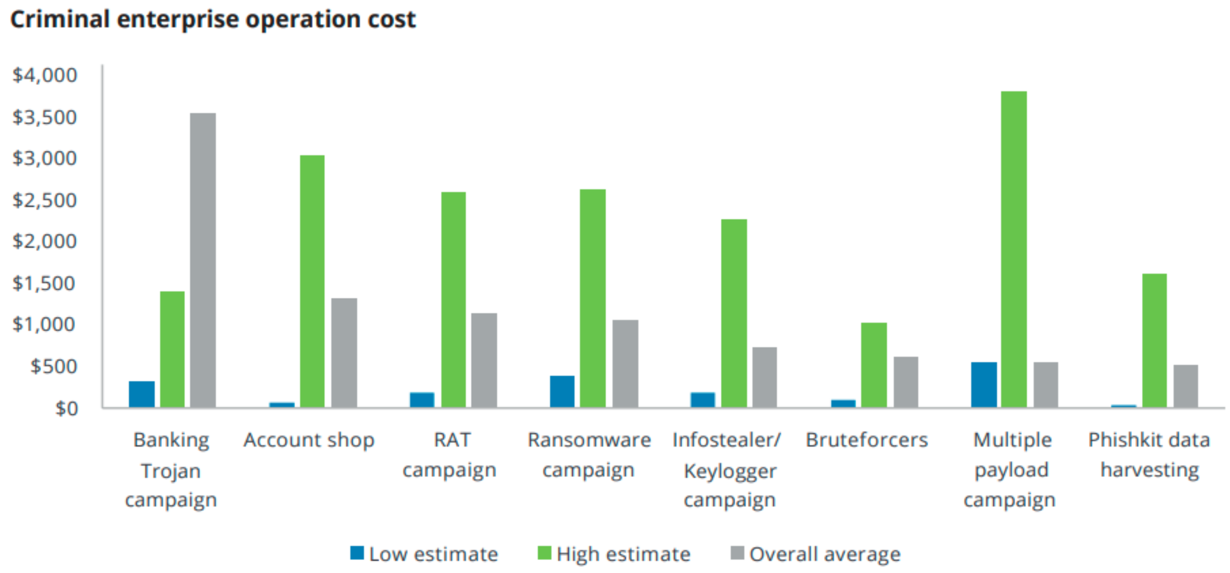


Figure 4
Source: 'Black Market ecosystem' - report by Deloitte

As is visible from Figure 3 and 4, a data breach can be quite profitable. The high profitability, the ease of access to the dark web, and the availability of 'hacking as a service' have led to an increase in breach incidents.

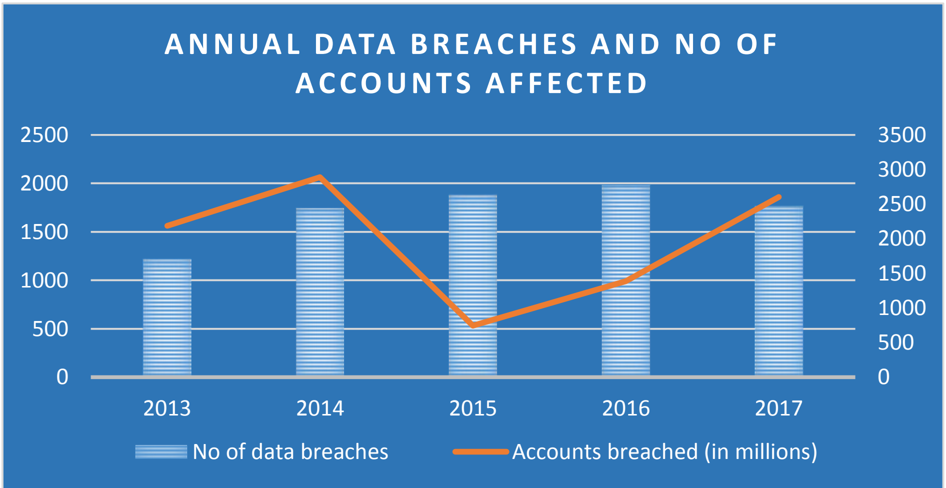


Figure 5. Source: https://www.apcela.com/blog/data-breach-statistics/

[6] https://www.kaspersky.com/about/press-releases/2019_number-of-users-attacked-by-banking-trojans-grew
[7] 500*70%*50% = 175
[8] https://www.thebalance.com/what-is-the-average-bank-account-balance-4171574

Cost of Data Breaches

India ranked fifth in the world in terms of the number of attacks initiated during 2013-2017 (the US ranked first).[9] In 2020, the average total cost of a breach in India was $2 million while the world average $3.86 million. However, the time taken to identify and contain a data breach in India is 318 days while the world took 280 days on average.[10] Apart from the detection and remedial costs, data breaches also result in loss of business, disruption of operations, loss of reputation and loss of employee confidence. Let us look at some examples of large data breaches of the past and what did they cost.

i. **LinkedIn**

In 2012 and again in 2016, around 107 million LinkedIn user accounts (6.5 million & 100 million respectively) were hacked and posted online for sale.[11] [12] LinkedIn has become a trusted forum for professional interaction, and a breach of this size can hamper this trust. LinkedIn sent change password emails to the affected accounts. For the 2012 breach, the company incurred more than $1 million towards forensic investigation and recovery cost alone.. An additional $2 - 3 million was spent on strengthening security. If we extrapolate the same cost for the 2016 fiasco, we get around $50 million in additional expenditure.

ii. Equifax

In 2017, Equifax, one of the largest credit bureaus in the US, disclosed that an application vulnerability in one of their websites exposed the personal data of about 163 million customers. The information included Social security number, date of birth, address, and driver's license number.[13] Such information leak can cause serious issues like identity theft for the owner. The company reached a settlement of $425 million with the FTC in January last year.[14]

iii. Multi-Specialty Private Hospital Chain

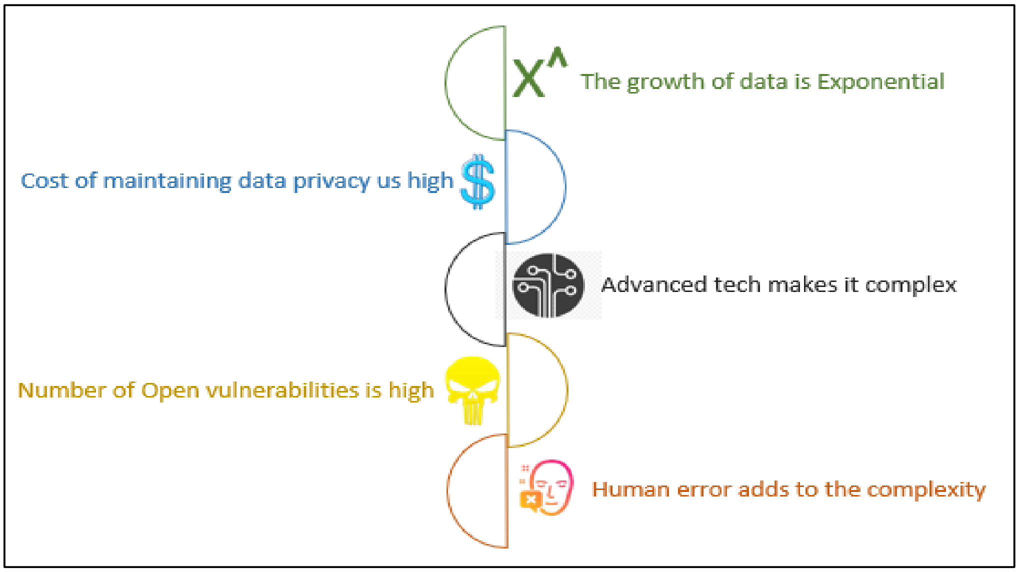
In an attack unprecedented in size, a large multi-specialty hospital in Kerala, India, had its complete patient records from the past 5 years exposed. The details included hundreds of test results and complete patient histories. The hospital also has one of the 101 NABL-accredited private labs in Kerala for RT-PCR testing resulting in a leak of a large number of COVID-19 test results also.[15]

[9] https://www.apcela.com/blog/data-breach-statistics/
[10] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[11] https://www.computerweekly.com/news/2240160962/LinkedIn-data-breach-costs-more-than-1m
[12] https://blog.linkedin.com/2016/05/18/protecting-our-members
[13] https://en.m.wikipedia.org/wiki/2017_Equifax_data_breach
[14] https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
[15] https://www.orfonline.org/expert-speak/data-privacy-pandemic-india-just-had-the-biggest-medical-records-breach-ever/

Healthcare remains the favorite target of hackers worldwide and even in each country. The average cost of a data breach is also higher: $7.13 million in healthcare.[16] One reason could be the price that a complete medical profile may be worth. While identification numbers and credit card info can fetch a few dollars, a complete medical information dossier can get prices anywhere between $300-$1000.[17, 18]

Regulations around Data Protection

One might ask a question that given the importance of data and its protection, why do organizations fail to protect it? The answer lies in the form of specific challenges that data protection presents.


X^
The growth of data is Exponential
Cost of maintaining data privacy us high
Advanced tech makes it complex
Number of Open vulnerabilities is high
Human error adds to the complexity

There are standards for data protection both in India and elsewhere.

i. In Indian context:

a) **Personal Data Protection Bill, 2019** – Still under consideration, one of the bill's highlights is the *right to be forgotten*, which provides for removing private information about a person from internet directories under certain circumstances. Critics, however, argue that this may result in the government taking control of people’s data in the name of public welfare.[19]

[16] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[17] https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/
[18] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/amp/
[19] https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill,_2019

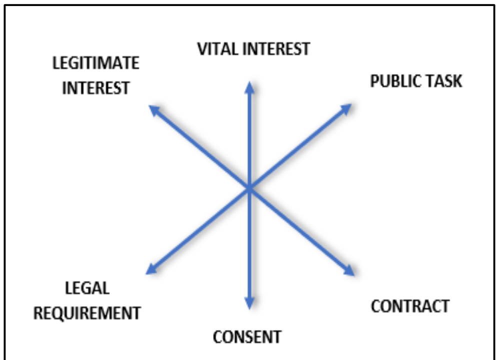
b) **Relevant sections of IT Act** – Section 43A provides compensation to anyone who has suffered a loss due to improper handling of their data by a body corporate. Section 72A, on the other hand, has provisions for the imprisonment of any person who inappropriately utilizes information gained during a work engagement.[20]

c) **Digital Information Security in Healthcare Act (DISHA)** – Still in the plans, DISHA makes the individuals the owners of their own healthcare data and lays down the purposes for which digital healthcare data can be collected and used by any entity.[21]

ii. In Global context:

a) General Data Protection Regulation (GDPR): GDPR was one of the first legislations to focus on general personal data security in the European Union and gives individuals control over their personal data. It provides six lawful bases under which any personal data may be processed and a fine of up to € 20 million for violation.[22]

b) **Payment Card Industry Data Security Standards (PCI-DSS):** It is a standard for organizations handling branded credit cards from major card schemes. Along with the requirements for protecting cardholder data, it also provides for Validation of Compliance, including a third-party audit.[23]



The Six bases for Data processing under GDPR
Source - Wikipedia

Best Practices

Your data is your property, and no one has the right to access or use it without your consent. Yet, just like in the case of your other properties, there would always be parties with mala-fide intentions wanting to gain at your expense. Still, there are certain things that both individuals and organizations could do to prevent such things from happening.

[20] https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d
[21] https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d
[22] https://en.m.wikipedia.org/wiki/General_Data_Protection_Regulation
[23] https://en.m.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

FOR IT & SECURITY TEAMS	FOR INDIVIDUALS
Train your employees on how to identify suspicious activity	Do not click on suspicious links or open email attachments from unknown senders
Find, classify, and protect your most sensitive data, particularly data covered under compliance regulations such as PCI-DSS	Use anti-malware software
Deploy patches as promptly as possible to shorten the vulnerability window	Update your software regularly for security patches
Employ data encryption to protect sensitive data in transit and at rest	Be cautious accessing online banking sites, email, or other sensitive sites, especially when using public connections
Monitor cloud usage, manage access to cloud services, and secure any data/applications during migration	Do not use the same password for multiple websites or services and allow a single compromised account to turn into many
Utilize security technologies such as anti-malware software and intrusion detection systems to build a shield around your environment	Consider using credit monitoring services to detect suspicious activity

Conclusion

We have seen that not even the largest organizations are entirely safe against the threat of data breaches, no matter how tight the security. While locks may deter the public from entering your house, they do not deter thieves. The financial incentives for data breaches (like every other major crime) are just too large. Still organizations must follow the given standards and adopt best practices so that the instances can be timely identified and even reduced to a greater extent.

****