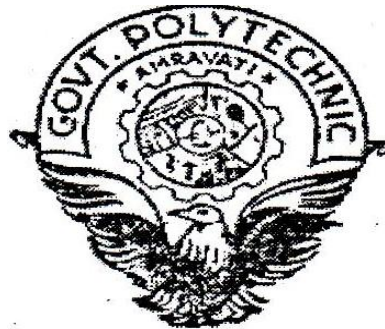


Seminar Report
On
**“Data Breach As The Top
Cyber Threat”**

**Submitted for partial fulfillment of requirement for the
Diploma in Computer Engineering**

Submitted By
Abhijeet S. Shahakar 18CM054
Under the Guidance of
Prof. V. M. Aswar



**Department of Computer Engineering,
Government Polytechnic Amravati**

(An Autonomous Institute of Government of Maharashtra)

2020-2021

CERTIFICATE

This is to certify that the Seminar entitled “Data Breach As The Top Cyber Threat” is a bonafide work and it is submitted to Government Polytechnic, Amravati

By

Abhijeet S. Shahakar

18CM054

in the partial fulfillment of the requirement for the Diploma in Computer Engineering, during the academic year 2019-2020 under my guidance.

Prof. V. M. Aswar

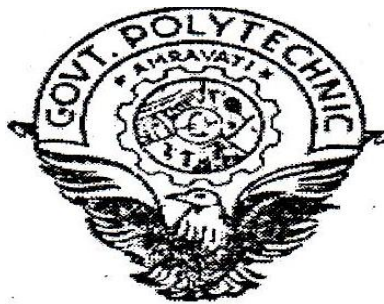
Guide

Department of Computer Engineering
Government Polytechnic, Amravati

Dr. P. S. Satav

Head

Department of Computer Engineering
Government Polytechnic, Amravati



**Department of Computer Engineering,
Government Polytechnic, Amravati**

(An Autonomous Institute of Government of Maharashtra)

2020-2021

ACKNOWLEDEMENT

It gives us immense pleasure in submitting the seminar report on topic “**Data Breach As The Top Cyber Threat**” to our guide **Prof. V. M. Aswar mam** who was a constant source of guidance and inspiration through developing the seminar report and for preparation of seminar.

I am also very thankful to all the staff members of Computer Engineering department, who have indirectly guided and helped me in preparation of this seminar.

We also express our sincere gratitude to our honourable principal **Dr. R. P. Mogre** sir for providing us necessary facilities.

At last I am thankful to my friends whose encouragement and constant inspiration helped us to for the preparation of the seminar.

Thanking You!

Abhijeet S. Shahakar (18CM054)

INDEX PAGE

Sr.No.	Title	Page No.
1.	Introduction	7
2.	What is targeted in data breaches?	7
3.	Malicious methods used to breach data.	9
4.	Reasons it happens.	10
5.	Top data breaches in history.	12
6.	How data breaches can be prevented.	15
7.	The damage a data breach can do.	16
8.	Technique to overcome a data breach	18
9.	Conclusion	20
10.	References	21

ABSTRACT

Today's technology is at its peak point beyond what we could ever imagine. New inventions and innovations are emerging on daily basis. In the path of developing technology many problems arises which have the potential of destroying successful companies, 'Data Breach' is one of them. A data breach is a security incident in which information is accessed without authorization. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair. From decades data breaches are consuming financial, technical resources. Data breaches are target at some specific areas of companies. Data collected from these areas is sold in black market on dark web. Various methods are used to do data breach attack. It costs companies to recover data and to resolve attack. Everyone must know ways to prevent data breaches on individual level. This problem cannot be solved permanently.

Hence, every user must have acknowledgement about hefty damage by data breaches. This acknowledgement will help industries to prevent it in future which will directly and indirectly provide better, secure and assured experience to users. Holding information about data breaches is necessary as computer science student.

Data Breach As The Top Cyber Threat

1. INTRODUCTION

To define data breach: a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission.

Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments. More importantly, anyone can put others at risk if they are not protected.

In general, data breaches happen due to weaknesses in:

- Technology
- User behaviour

As our computers and mobile devices get more connective features, there are more places for data to slip through. New technologies are being created faster than we can protect them. Devices in the IOT sector are proof that we are increasingly valuing convenience over security.

Many “smart home” products have gaping flaws, like lack of encryption, and hackers are taking advantage. Since new digital products, services, and tools are being used with minimal security testing, we’ll continue to see this problem grow.

However, even if the backend technology was set up perfectly, some users will likely still have poor digital habits. All it takes is one person to compromise a website or network. Without comprehensive security at both the user and enterprise levels, you are almost guaranteed to be at risk.

2. WHAT IS TARGETED IN DATA BREACHES?

Although a data breach can be the result of an innocent mistake, real damage is possible if the person with unauthorized access steals and sells Personally Identifiable Information (PII) or corporate intellectual data for financial gain or to cause harm.

Malicious criminals tend to follow a basic pattern: targeting an organization for a breach takes planning. They research their victims to learn where the vulnerabilities are, such as missing or failed updates and employee susceptibility to phishing campaigns.

Hackers learn a target's weak points, then develop a campaign to get insiders to mistakenly download malware. Sometimes they go after the network directly. Once inside, malicious criminals have the freedom to search for the data they want — and lots of time to do it, as the average breach takes more than five months to detect.

Common vulnerabilities targeted by malicious criminals include the following:

Weak credentials: The vast majority of data breaches are caused by stolen or weak credentials. If malicious criminals have your username and password combination, they have an open door into your network. Because most people reuse passwords, cybercriminals can use brute force attacks to gain entrance to email, websites, bank accounts, and other sources of PII or financial information.

Stolen credentials: Breaches caused by phishing are a major security issue and if cyber criminals get hold of this Personal information, they can use it to access things like your bank and online accounts

Compromised assets: Various malware attacks are used to negate regular authentication steps that would normally protect a computer.

Payment Card Fraud: Card skimmers attach to gas pumps or ATMs and steal data whenever a card is swiped.

Third-party access: Although you may do everything possible to keep your network and data secure, malicious criminals could use third-party vendors to make their way into your system.

Mobile Devices: When employees are allowed to bring their own devices (BYOD) into the workplace, it's easy for unsecured devices to download malware-laden apps that give hackers to data stored on the device. That often includes work email and files as well as the owner's PII.

3. MALICIOUS METHODS USED TO BREACH DATA

Since malicious data breaches result from cyber attacks, you should know what to watch for. Here are some popular methods used by hackers

- Phishing
- Brute Force Attacks
- Malware

Phishing: These social engineering attacks are designed to fool you into causing a data breach. Phishing attackers pose as people or organizations you trust to easily deceive you. Criminals of this nature try to coax you into handing over access to sensitive data or provide the data itself.

Brute force attacks: In a more brash approach, hackers might enlist software tools to guess your passwords. Brute force attacks work through all the possibilities for your password until they guess correctly. These attacks take some time but have become rapid as computer speeds continue to improve. Hackers even hijack other devices like yours via malware infections to speed up the process. If your password is weak, it might only take a few seconds to crack it.

Malware: Your device's operating system, software, hardware, or the network and servers you're connected to can have security flaws. These gaps in protection are sought out by criminals as the perfect place to shove malware into. Spyware specifically is ideal for stealing private data while being completely undetected. You might not find this infection until it's too late.

4. REASONS IT HAPPENS

Cause #1: Old, Unpatched Security Vulnerabilities

For years, information security specialists have been compiling information on the exploitations that hackers have successfully used on companies in dozens of countries. These exploits are sorted into hundreds of Common Vulnerabilities and Exposures (CVEs) to identify them for future reference.

Leaving these old security vulnerabilities unfixed gives hackers a free pass to your company's most sensitive information.

Cause #2: Human Error

Unfortunately, one of the biggest sources of a data breach isn't some unknown or forgotten security bug, its human error.

According to statistics from a CompTIA study cited by shrm.org, "Human error accounts for 52 percent of the root causes of security breaches." The specific nature of the error may vary, but some scenarios include:

- The use of weak passwords;
- Sending sensitive information to the wrong recipients;
- Sharing password/account information; and
- Falling for phishing scams.

Cause #3: Malware

Malware isn't just a problem for personal computers at the homes of employees, it's an ever-expanding threat aimed directly at your company's systems. According to the Verizon DBIR 2015, "5 malware events occur every second."

While many of these “malware events” are minor in nature, the sheer number of these events can be worrying.

Also, there exists an incredible amount of variation between malware samples. As pointed out in the Verizon DBIR, “we found that 70 to 90% (depending on the source and organization) of malware samples are unique to a single organization.”

Despite this fact, many malware programs hail from just a few different “families.” According to Verizon, “20 families represented about 70% of all malware activity.”

Why? The main reason is that many hackers make minor modifications to existing malware programs to try and make them unrecognizable to antivirus programs while still producing the intended effect by the hacker.

Cause #4: Insider Misuse

While closely related to human error, this cause of company data is more insidious in nature. Human error implies an innocent accident or mistake. Insider misuse, on the other hand, is the deliberate abuse of your company’s systems by an authorized user, typically for personal gain.

As pointed out in Verizon’s 2015 DBIR, “it’s all about grabbing some easy Benjamins for these mendacious malefactors, with financial gain and convenience being the primary motivators (40% of incidents).”

The issue here is that the malicious actor is someone in whom your organization has placed trust. Worse yet, as pointed out by Verizon’s report, “catching insider abuse is not easy... in many of the incidents we reviewed, the insider abuse was discovered during forensic examination of user devices after individuals left a company.”

While preventing insider abuse is nearly impossible, damage can be limited through compartmentalization of information on your network or cloud. The fewer files and systems

a single user can access, the harder it is for them to abuse their access. However, it can also make sharing of necessary data more difficult as well.

Cause #5: Physical Theft of a Data-Carrying Device

Last on this list, but not the least-threatening, is the physical theft of a device that holds your company's sensitive information. This can include laptops, desktops, smartphones, tablets, hard drives, thumb drives, CDs & DVDs, or even servers.

The severity of a data breach from a stolen device depends largely on the nature of the information stored on the device. More sensitive info generally equals a more severe data breach if the device is stolen without being wiped.

According to the Verizon report, "most of the theft occurred within the victim's work area (55% of incidents), but employee-owned vehicles (22% of incidents" are also a common location for thefts to occur."

Most of these thefts are opportunistic in nature, making them difficult to predict. The best solution is often to reduce the opportunities for removing data-storing devices from the work site.

5. TOP DATA BREACHES IN HISTORY

1) CAM4 data breach



Date: March 2020

Impact: 10.88 billion records.

Adult video streaming website CAM4 has had its Elastic search server breached exposing over 10 billion records. The breached records included the following sensitive information:

- Full names
- Email addresses
- Sexual orientation
- Chat transcripts
- Email correspondence transcripts
- Password hashes
- IP addresses
- Payment logs

Many of the exposed email addresses are linked to cloud storage services. If hackers were to launch successful phishing attacks on these users, they could gain deeper access to personal photos and business information.

Due to the licentious connection of the breached database, compromised users could fall victim to blackmail and defamation attempts for many years to come.

2) Yahoo data breach 2017



Date: October 2017

Impact: 3 billion accounts

Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo while in negotiations to sell itself to Verizon, on December 14, 2016, and forced all affected users to change passwords, and to reenter any unencrypted security questions and answers to make them encrypted in the future.

However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.

3) Aadhaar data breach



Date: March 2018

Impact: 1.1 billion records

In March of 2018, it became public that the personal information of more than a billion Indian citizens stored in the world's largest biometric database could be bought online.

This massive data breach was the result of a data leak on a system run by a state-owned utility company. The breach allowed access to private information of Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and their bank details.

The type of information exposed included the photographs, thumbprints, retina scans and other identifying details of nearly every Indian citizen.

6. HOW DATA BREACHES CAN BE PREVENTED

- 1) **Limit access to your most valuable data:** In the old days, every employee had access to all the files on their computer. These days, companies are learning the hard way, to limit access to their more critical data.
- 2) **Conduct employee security awareness training:** According to recent surveys, employees are the weakest link in the data security chain.
- 3) **Update software regularly:** Professionals recommend keeping all application software and operating systems updated regularly.
- 4) **Develop a cyber breach response plan.**
- 5) **Difficult to decipher passwords.**
- 6) **High-grade encryption** for sensitive data.
- 7) **Enforcing BYOD security policies**, like requiring all devices to use a business-grade VPN service and antivirus protection.
- 8) **Enforcing strong credentials and multi-factor authentication** to encourage better user cybersecurity practices. Encouraging users to start using a password manager can help.

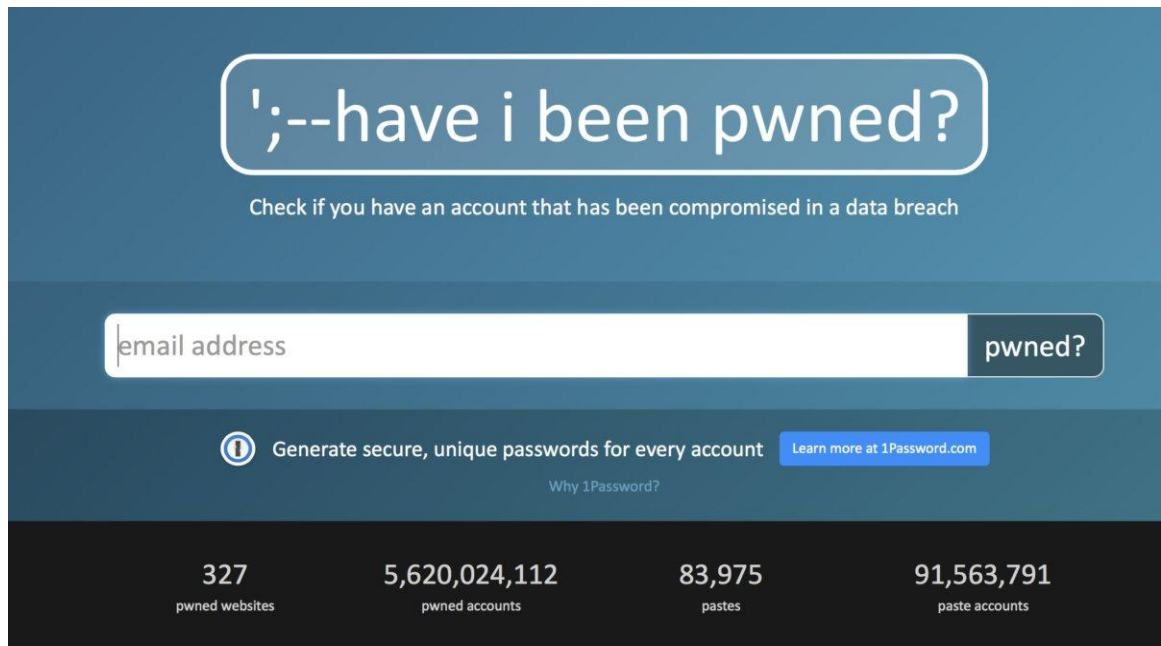
- 9) **Educating employees** on best security practices and ways to avoid socially engineered attacks.

7. THE DAMAGE A DATA BREACH CAN DO

In many cases, data breaches cannot just be patched up with some password changes. The effects of a data leak can be a lasting issue for your reputation, finances, and more.

- 1) **For business organizations:** a data breach can have a devastating effect on an organization's reputation and financial bottom line. Organizations such as Equifax, Target, and Yahoo, for example, have been the victims of a data breach. And today, many people associate/remember those companies for the data breach incident itself, rather than their actual business operations.
- 2) **For government organizations:** compromised data can mean exposing highly confidential information to foreign parties. Military operations, political dealings, and details on essential national infrastructure can pose a major threat to a government and its citizens.
- 3) **For individuals:** identity theft is a major threat to data breach victims. Data leaks can reveal everything from social security numbers to banking information. Once a criminal has these details, they can engage in all types of fraud under your name. Theft of your identity can ruin your credit, pin you with legal issues, and it is difficult to fight back against.

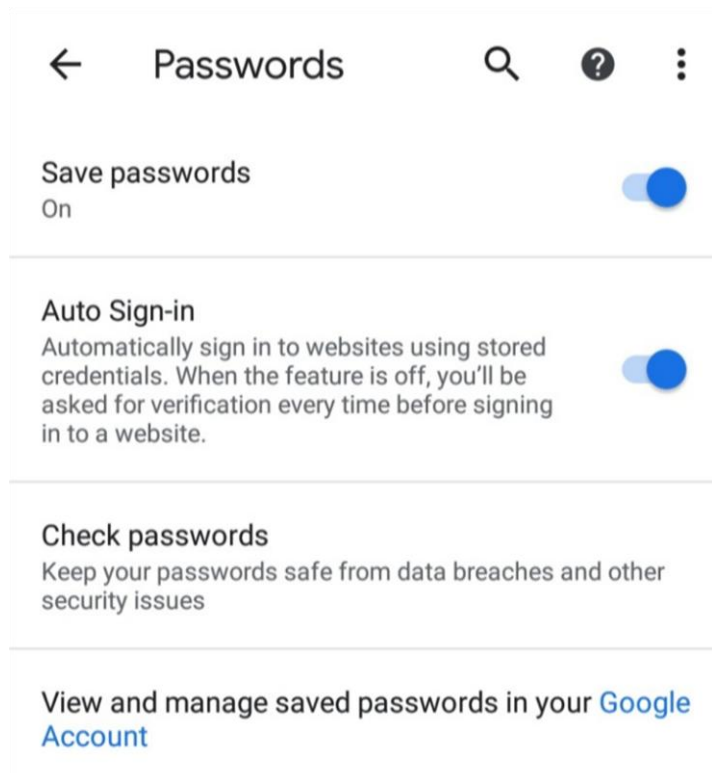
While these are common cases, the harm done by data breaches can extend far beyond these situations. So, it is essential that you investigate whether your data has already been exposed.



The screenshot shows the homepage of the 'have i been pwned?' website. At the top, the title is enclosed in a rounded rectangle. Below it is a subtitle. A search bar with the placeholder 'email address' and a 'pwned?' button is present. A banner for 1Password is shown below the search bar. At the bottom, four statistics are listed in a grid.

Category	Count
pwned websites	327
pwned accounts	5,620,024,112
pastes	83,975
paste accounts	91,563,791

To find out if your personal or work accounts have been compromised use <https://haveibeenpwned.com/> to check (this tool checks existing data breaches for your email address and reports what was leaked).



Chrome browser of Google notifies you when your saved passwords are compromised in a data breach. The only condition is to use chrome's password manager.

8. TECHNIQUE TO OVERCOME A DATA BREACH

1) Stop the breach

Once an organization notices a breach, it's important to contain the breach as quickly as possible. Once it's been contained, it's important to eliminate the threat to prevent any further damage. Methods for eradication of the attack vary depending on the type of attack itself.

2) Assess the damage

Once the attack has been stopped and eliminated, the next step is to investigate it and assess the damage it has caused to the organization.

.

During the assessment, information that should be dug up includes:

- What was the attack vector?
- Was the attack based on social-engineering tactics or through user accounts?
- How sensitive is the breached data?
- What is the type of that data affected?
- Does the data contain high-risk information?
- Was the data encrypted and can it be restored (did the company backup their data)?

3) Notify those affected

After the investigation, the next step is to notify authorities, third-party organizations and any individuals who might be affected. Since regulations govern the time frame in which the breach needs to be reported, it's always best to do it as soon as possible. The notification can be distributed via email, mass email, phone calls or any other mediums of communication you typically use with the affected parties.

4) Security audit

A security audit is needed to assess the organization's current security systems and to help with preparation for future recovery plans.

An audit after a data breach or similar event needs to analyze the situation and all systems so that a proposition for implementing new fixes and policies can be provided. As for a security audit routine that companies should enforce, a DNS Audit will help secure the entire infrastructure and system administration, since an outdated DNS server can enlarge the attack surface

5) Update your recovery plan to prepare for future attacks

After an attack and taking all the appropriate steps for recovery, the importance of preparing for the next attack can't be stressed enough. After being attacked once, the possibilities that you will be attacked again are substantial; it's possible that the same attacker or group of attackers will try it again since they've already succeeded, or other groups will use the same or similar methods.

CONCLUSION

Today we are totally dependent on technology for day to day task. Our daily life, job, entertainment is based on technology. With the growing nature of technology we need to understand the importance of cyber security and our duty towards cyber security. Spreading awareness to prevent cyber crime is the prime task for us as we are from computer science background. This report spread awareness among students about the biggest cyber threat 'Data Breaches' which is damaging internet from decades. Every computer science student must have knowledge about data breaches, its advantages, disadvantages, what we can learn from data breaches, how to prevent it, how it is possible, which methods are used to make it happen and how much damage it can make. As computer engineering student it is necessary to have knowledge about 'Data Breaches'. This problem can't be solved permanently and technology can't be 100% secure.

Hence, every user must have acknowledgement about hefty damage by data breaches. This acknowledgement will help industries to prevent data breaches in future which will directly and indirectly provide better, secure and assured experience to users. Holding information about data breaches is necessary as computer science student.

REFERENCES

- [1] <https://www.upguard.com/blog/biggest-data-breaches>
- [2] <https://usa.kaspersky.com/resource-center/definitions/data-breach>
- [3] https://en.wikipedia.org/wiki/Data_breach
- [4] <https://www.csoononline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>
- [5] <https://www.cshub.com/attacks/articles/top-cyber-security-breaches-an-overview-of-q2-2020-incidents>
- [6] <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/>
- [7] <https://www.whoa.com/data-breach-101-top-5-reasons-it-happens/>