Project : - 2

Project Name : - Investigation of a Data Breach

Objective: Investigation of a Data Breach on a Renowned Website.

Introduction

What is a Data Breach?

Ans : - A data breach refers to an incident in which secure, sensitive, and confidential information is accessed and exposed to an unauthorized and untrusted environment. The breach can be intentional or accidental. Technically, a data breach is a violation of security protocol for an organization or individual in which confidential information is copied, transmitted, viewed, and stolen by an unauthorized person .

Project : - 2

Data breaches involve theft or loss of private information, such as:

- Financial data (credit card, banking details)
- Personal medical data history
- Personal identification information (passwords, PIN (personal identification number), Social Security number)
- Trade secrets
- Contact details (names, physical addresses, e-mails)
- Intellectual information

Data breaches are a common occurrence due to technological advancement and the sheer amount of information in digital form. They are largely carried out by cybercriminals or hackers for financial gain, espionage, terrorism, politics, or other reasons. Data breaches can potentially ruin the reputation of prominent organizations, destroy lives, and can be costly to remedy through costs of investigation, redress, victim compensation, fines, etc.

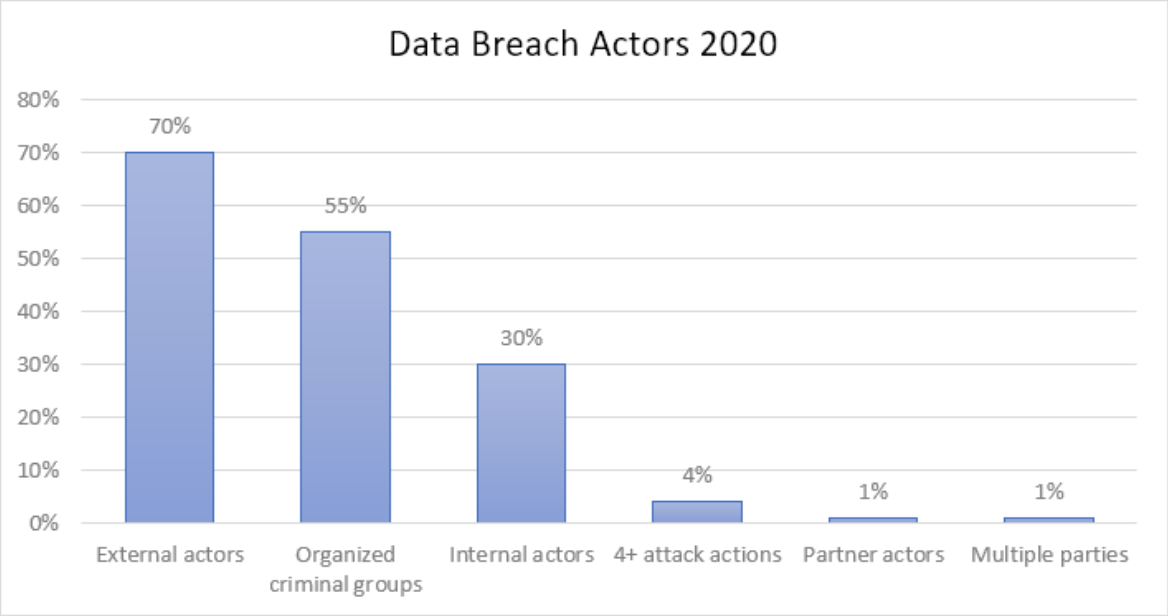
How Data Breaches Occur

Data breaches, in general, occur due to weaknesses in systems and user behavior. Hackers are always looking to exploit the deficiencies. The rise of smartphones and social media led to the interconnectedness of devices, and constant technology upgrades are happening faster than the protection against them. In essence, more value is being placed on convenience rather than security, and it inevitably leads to more incidences of data breaches. The following are some of the ways in which data breaches occur:

- **Accidental internal breach**: Where an employee can gain access to information from another colleague at the workplace or view information on the manager's computer without authorization. The employee may not share the information with anyone, but because they accessed and viewed the information without authorization, it is classified as a data breach.

- **Intentional internal breach**: Where an employee accesses and views company data with or without authorization but with intent to share it with unauthorized outsiders or other employees to cause harm and profit from the breach action.
- **Physical loss or theft of devices**: Where devices with sensitive unencrypted information are lost or stolen, risking exposure to unintended parties.
- **Cybercrime**: Where cybercriminals or hackers take time to study and gather intel about an organization's information system before launching an attack to breach and steal information for nefarious reasons.

According to the 2020 Verizon Data Investigations Report (DBIR 2020), external actors were the major perpetrators behind 70% of data breaches. The chart below summarizes threat actors in 2020



Targeted Cyber Attacks

Targeted data breaches carried out by cybercriminals and hackers continue to increase despite the implementation of measures to counter them. Their ultimate goal is to steal personal identification

information and compromise identities for financial gain by selling information on the dark web. The following are the main ways in which targeted attacks can happen:

- **Weak passwords**: It is easy to detect weak passwords to gain access to important sensitive information. They are commonly simple passwords that contain whole words that are common or known personal information, such as date of birth or that of a close relative. People generally want simple passwords that are easy to remember, and hackers know that and exploit them.
- **System vulnerabilities**: Obsolete firewalls and out-of-date software create vulnerabilities in the system, which open up opportunities for hackers to sneak malware into the system to steal data.
-
- **Malware attack**: Targeted malware attacks make use of spam and phishing emails to mislead users to reveal their network credentials. Users can be forced to download attachments with malware or redirected to a malicious website through spam. Malware exploits weaknesses in hardware and software security. Spyware is a type of malware used to steal data while remaining undetected.
-
- **Drive-by download**: Involves misleading users to unintentionally download malware by visiting compromised websites. It happens through exploiting out-of-date browsers, applications, and operating systems.
-
- **Phishing**: Attacks are aimed at deceiving users to hand over credentials or data by pretending to be bona fide people or organizations.
-
- **Brute force attacks**: Software tools used by hackers to guess user passwords. It can take time to guess it correctly depending on the password strength, but with higher processing speeds and malware infections, the process can be speeded up.

Project : - 2

Current Data Breach Methods

The DBIR 2020 lists nine core clusters of incidence classification patterns, which account for about 88% of data breaches. They are the common ways in which data breach incidences were occurring in 2020. However, these actions remain fairly consistent year over year, with slight deviations depending on technology. The nine common clusters include:

- **Crimeware** – Includes all malware not classified under other patterns. Crimeware methods often tend to be opportunistic and financially motivated. Malware is a form of social engineering which uses malicious software. It includes the following sub-units:
    - **Ransomware** – As the name suggests, the method holds the target files hostage with a promise to unlock them if the victim pays. The challenge for the victim is that files might not get unlocked even after paying the ransom.
    - **SQL injection** – A hacker places a code into an online web user form which can corrupt the website if the form is not handled properly when it passes through the backend database.
    -
    - **Phishing** – The hacker poses as a trusted source to the intended victim, normally through email, text, chat, or direct phone call. Once the victim accepts the mode of contact, they will be literally installing malware or sharing personal information without realizing it.
    -
- **Cyber espionage** – Data breach incidents involving unauthorized system access of state secrets on countries and states.
- **Denial of service** – Involves criminals sending junk network traffic to overwhelm systems and networks. It results in services being denied and disrupted as the system cannot differentiate or handle both incoming illicit and authentic traffic.
- **Privilege misuse** – Intentional actions carried out by company insiders or employees. Employees will likely know the value of the data and trade it for profit clandestinely.

- **Miscellaneous errors** – Unintentional actions that result in a data breach. It can happen by accident or through the loss of devices containing sensitive, confidential data.
- **Payment card skimmers** – Incidents where a skimmer or skimming device is used to acquire payment data from a credit card reader or any terminal, e.g., ATM and gas pump terminals.
- **Point of Sale (PoS)** – Involves hacking and remote intrusions into PoS servers and terminals to steal payment card details. It mostly targets small businesses and retail customers.
- **Lost and stolen assets** – Intentional or accidental theft or loss of devices containing sensitive information. It can involve losing physical devices, such as laptops, cell phones, or paper documents.
- **Web applications** – Includes any attack that involves using web applications where personal details are shared. Cyber-criminals attack the code of the web application, e.g., code-based vulnerabilities. The purpose is to steal personal details and credentials for use elsewhere.
- **Everything else** – All other methods not contained in the above categories. It normally includes phishing, compromised email accounts with the intention to commit fraud for financial reasons.

Data Breach Prevention

It is said that the security of a network is only as strong as its weakest link. Hence, it is crucial that individuals and organizations put in place inclusive preventative measures to close all potential system vulnerabilities from IT systems to end-users. Methods to prevent and minimize data breach impact include:

- Regularly patching and updating software
- Conducting regular vulnerability and penetration testing

- Encryption of sensitive data on the local onsite network, as well as third-party cloud services. This ensures that even in the event of network penetration, threat actors will not be able to decrypt or access the actual data.
- Use of strong antivirus protection, which should be regularly updated.
- Enforcing strong credentials and multi-factor authentication.
- Ensuring all devices use business-grade VPN services.
- Formulation and circulation of data security policy for all employees
- Continuous education and refresher training of staff on cybersecurity best practices, as well as the promotion of data security policy
- Establishing Principle of Least Privilege (POLP) where employees are given the least possible permission and rights to undertake their work.
- Formulating an Incident Response Plan (IRP) to be implemented in the event of a data breach incident. The IRP contains processes to be followed from identification, controlling, and quantifying a security incident.

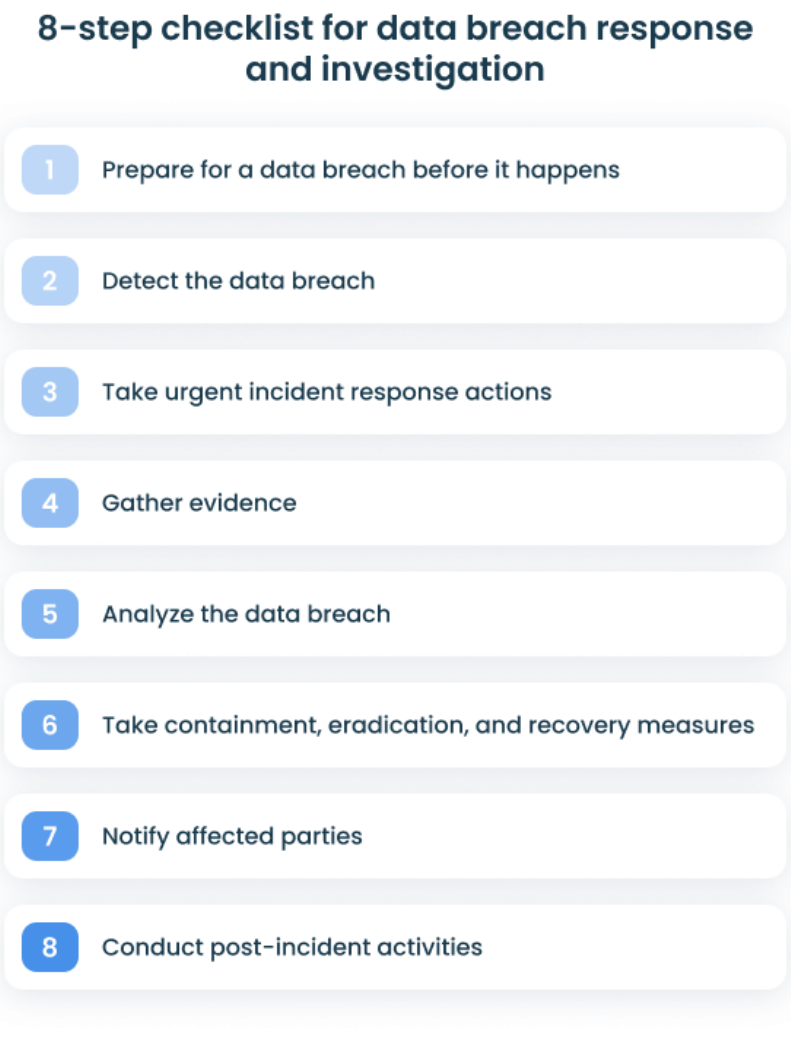
Data Breach Incident Cases

There are several data breaches that have taken place since the turn of the century, and many more keep being reported. As indicated earlier, the migration of world economies and corporations to the digital age creates exposed flaws in security systems. The large volume of government and corporation data appeals to criminals to benefit financially and for espionage purposes.

Project : - 2

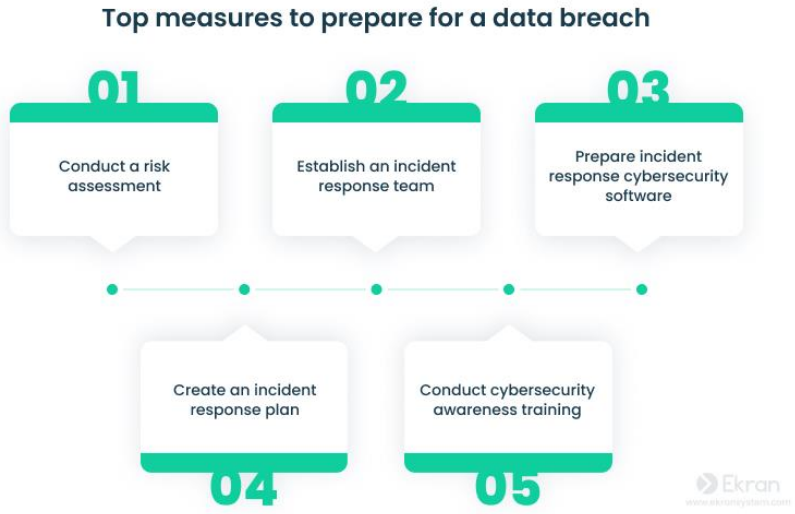
Tools and techniques used for investigation.

8 key steps for data breach response and investigation Although the reasons behind a data breach may vary, there are strict steps you need to take when responding to and investigating any such cybersecurity incident.



Project : - 2

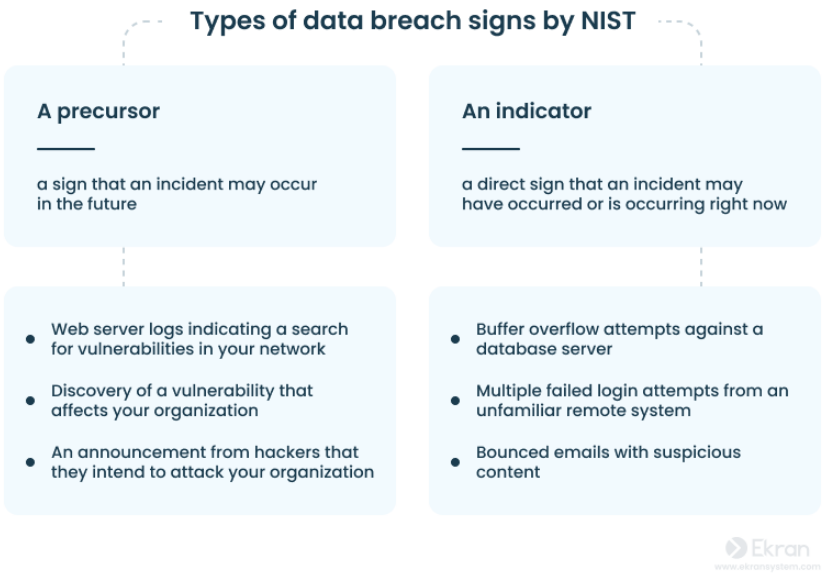
1. Prepare for a data breach before it happens Your organization should be ready to handle a data breach before it happens. Good preparation can significantly reduce the risk of business damage and simplify your response and recovery processes.



Preparation involves assessing the risks, establishing an incident response team, and, eventually, creating an incident response plan (IRP). An IRP can coordinate your organization if a data breach happens and take proper first steps to investigate and remediate it. An essential part of the preparation process is obtaining all necessary technological resources to ensure data security and respond to data breaches: threat detection and monitoring tools, data loss prevention systems, access management solutions, user and entity behavior analytics (UEBA) software, etc. To prevent a data breach from happening in the first place, consider treating your employees as your main line of defense. You can do so by conducting regular cybersecurity training. In training sessions, explain what data breach risks there are, what attack techniques cybercriminals use, and what your employees should do to ensure reliable data security.

Project : - 2

Detect the data breach All tips for investigating a data breach begin with data breach detection measures. This step is aimed at determining the fact that a data breach has occurred. Not sure how to detect data breaches? Look for their signs. In the Computer Security Incident Handling Guide [PDF], NIST distinguishes two types of data breach signs: precursors and indicators.



The structured MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) knowledge base can also be of great help. It describes known attacker behaviors, divided into tactics and techniques and expressed in tables (matrices). The MITRE ATT&CK

model for threat mitigation provides a comprehensive view of attackers' behavior and is extremely useful for data protection, monitoring, and employee training ,

2. Take urgent incident response actions You should take several urgent steps when a data breach is detected. The first is to record the date and time of detection as well as all information known about the incident at the moment. Then, the person who discovered the breach must immediately report to those responsible within the organization. Security officers should also restrict access to breached information to prevent the further spreading of leaked data.

3. Gather evidence Make sure to gather data from all your cybersecurity tools, servers, and network devices and to collect information from your employees during interviews. Act quickly and gather as much information about the data breach as you can. The better your understanding of the situation, the better your chances of minimizing the consequences

5. Analyze the data breach Once you've

gathered information about the incident, you need to analyze it. This step aims to determine the circumstances of the incident.

6. Take containment, eradication, and recovery measures It's essential to prevent the data breach from spreading and be able to restore your organization's operations. You can accomplish this with three countermeasures: containment, eradication, and recovery. Containment. The goal of this measure is not only to isolate compromised computers and servers but also to prevent the destruction of evidence that can help investigate the incident. Conduct a comprehensive data breach containment operation and preserve all evidence. Also, monitor the attacker's activities and determine whether any data is leaking during the investigation. Eradication. Eliminating all causes of the data breach is essential. For example, if the breach occurred because of an insider threat, security specialists should disable all accounts that leaked information. If the threat was external, such as malware, it may be necessary to clean up the affected system and patch exploited vulnerabilities. Recovery. After successful eradication, the organization must restore normal operations. This includes returning the affected systems to a fully operational state, installing patches, changing passwords, etc. Security specialists should carefully monitor the network, recovered computers, and servers to ensure that the threat no longer exists

7. Notify affected parties Regardless of whether you're legally obliged to do so, consider notifying all affected organizations, individuals, and law enforcement. Timely notification is vital, as it will enable individuals to take protective measures, such as changing passwords, or at least to be careful in case scammers take advantage of the data breach.

8. Conduct post-incident activities Once you've taken actions to counter the data breach, it's time to analyze the incident and its consequences and take measures to prevent similar issues in the future. Every data breach should be thoroughly audited afterward. The specifics of each audit depend on the data breach itself and its cause

Conclusion : - Preparing to respond to and investigate data breaches in a timely manner will strengthen your business continuity and enhance your cybersecurity in general.

Project : - 2

Thanks Extion infotech

Submitted by – RAHUL SAHU

Email – rahulsahurs403@gmail.com