Investigation of a Data Breach

Report: Data Breach Analysis of Yahoo (2013)

The 2013 Yahoo Data Breach Attack was one of the biggest data breaches ever seen in the history of mankind or the cyber world. This breach attack had a devastating effect for around 3 billion people and even more, where it has been considered, the single most, point blank, brute attack on the internet, showcasing a widespread havoc and weakness of the internet on daily usage.

The reason for this topic and investigation is to re-modelise the lifestyle we are living through the internet and making sure its a constant reminder that the internet is nothing but a spontaneous friend and foe, based on the perspective and usage.

---

1. Incident Analysis:

Breach Overview:

In 2013, Yahoo experienced one of the largest data breaches in history, compromising data from all three billion of its user accounts. This breach was discovered and disclosed years later in 2016 during Yahoo’s acquisition negotiations with Verizon. The attackers gained access to Yahoo's network and exfiltrated vast amounts of sensitive user data.

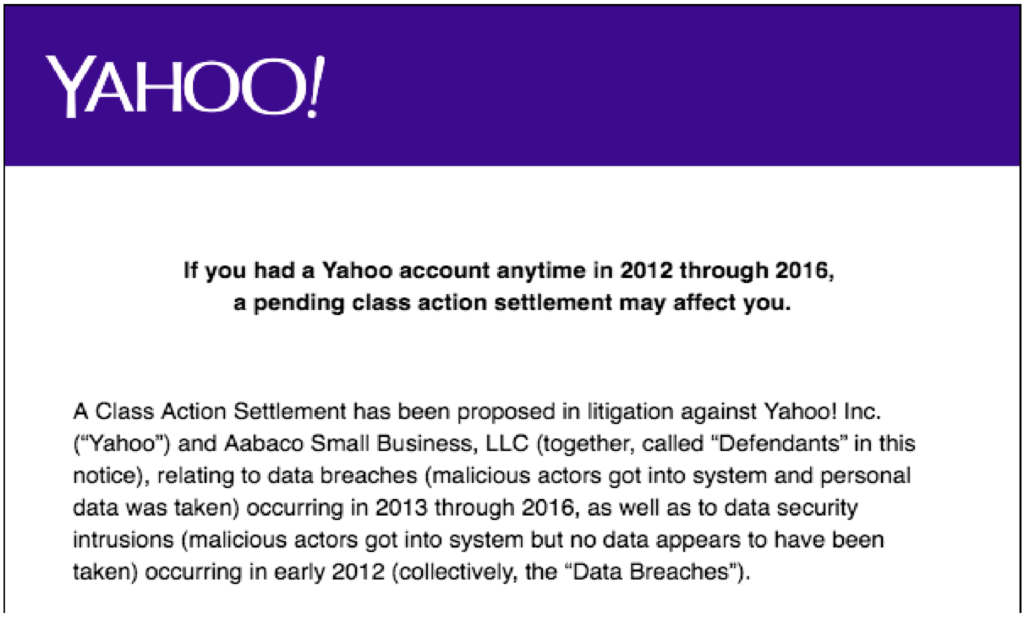
Point of Entry:

- The breach exploited vulnerabilities in Yahoo’s proprietary code for account management. This suggests a flaw in the infrastructure and weak datapoint security in Yahoo and its connected services.
- Attackers leveraged stolen credentials obtained via phishing or other social engineering techniques. This was taken as an attack vector and used to deliver other forms of attacks to target end users using various objectives.
- The main frame of weakness was found through its weak encryption protocols and an outdated security posture, which made it easier for attackers to persist in Yahoo's systems undetected.

Timeframe:

- The breach is believed to have occurred in late 2013.
- Yahoo did not detect the breach until years later, showing a lack of robust incident detection mechanisms.
- It took around 3 to 4 solid years of interceptions and keen analysis to interject, to properly find the method of attack, without the valid source, unfortunately.

An Explicit Way to Inform Users about the attack.



**If you had a Yahoo account anytime in 2012 through 2016,
a pending class action settlement may affect you.**

A Class Action Settlement has been proposed in litigation against Yahoo! Inc. (“Yahoo”) and Aabaco Small Business, LLC (together, called “Defendants” in this notice), relating to data breaches (malicious actors got into system and personal data was taken) occurring in 2013 through 2016, as well as to data security intrusions (malicious actors got into system but no data appears to have been taken) occurring in early 2012 (collectively, the “Data Breaches”).

Extent of Breach:

- All three billion user accounts were impacted.
- Exposed data included PIIs (Personally Identifiable Information), and at worst cases SPIIs (Sensitive Personally Identifiable Information) such as:
  - Usernames
  - Email addresses
  - Telephone numbers
  - Birthdates
  - Hashed passwords (using MD5, a weak and outdated hashing algorithm)
  - Encrypted or unencrypted security questions and answers.

---

2. Forensic Analysis:

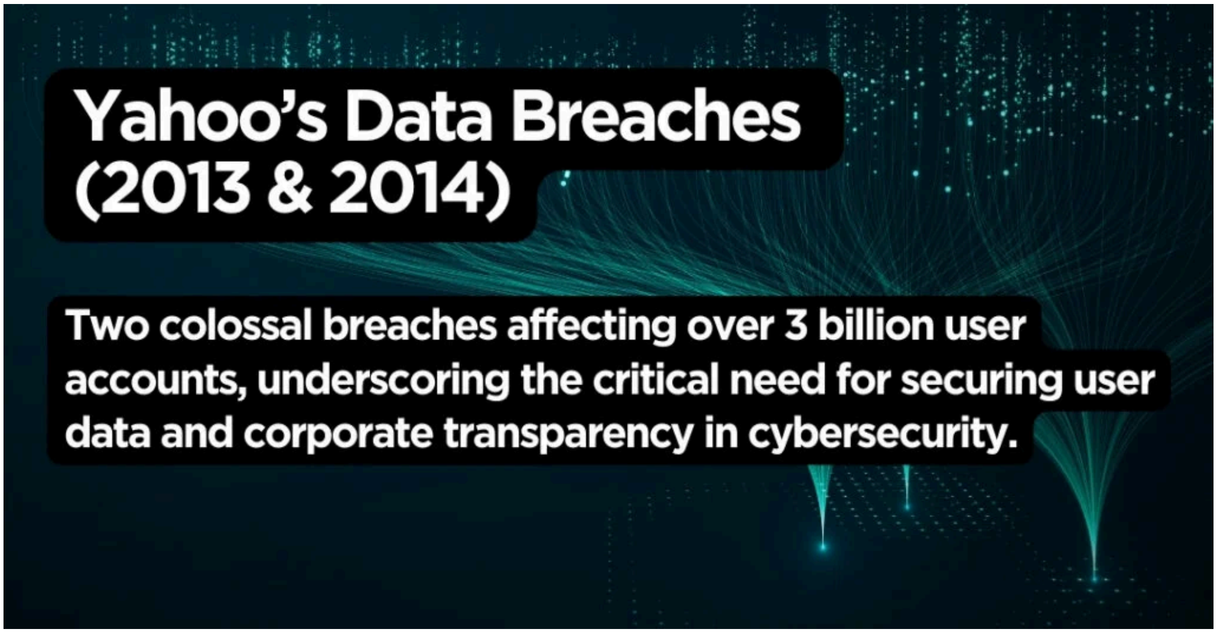
Forensic Investigation Findings:

- Attackers installed malware on Yahoo's servers to maintain access and exfiltrate data.
- Analysis revealed that the encryption used for passwords (MD5) was highly vulnerable to brute force attacks, allowing attackers to crack the hashed passwords.
- Logs and metadata indicated persistent lateral movement by attackers, showing a lack of network segmentation.
- Evidence pointed to the involvement of state-sponsored actors, as noted in Yahoo's public statements.

Malware Analysis:

- Malware used included custom backdoors for remote access and data extraction.
- The attackers employed anti-forensic techniques to erase traces, delaying breach discovery.

What can be the limits of hackers, when they have the vector at hand!



Yahoo's Data Breaches (2013 & 2014)

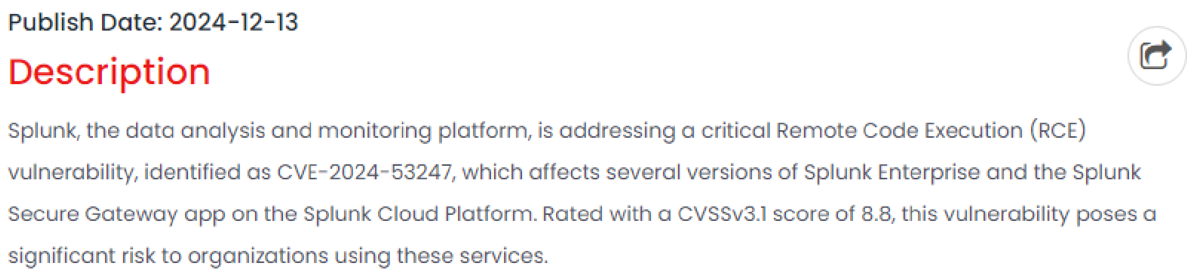
Two colossal breaches affecting over 3 billion user accounts, underscoring the critical need for securing user data and corporate transparency in cybersecurity.

Tools and Techniques Used in Forensic Analysis:

- Log analysis software (e.g., Splunk) to identify unauthorized access patterns.
- Network monitoring tools to reconstruct the attackers' movements within Yahoo's infrastructure.
- File integrity monitoring to identify modified files and planted backdoors.

The findings of the Splunk:

1. **Log Analysis**: Aggregating and correlating logs from different systems to identify suspicious login attempts and unusual activities within Yahoo's infrastructure.
2. **Identifying Unauthorized Access**: Pinpointing the exact times and locations of unauthorized access to Yahoo's systems.
3. **Tracing Lateral Movement**: Mapping the attackers’ movement across Yahoo's network to uncover how they navigated between systems and maintained persistent access.
4. **Detecting Malware Activity**: Identifying indicators of compromise (IoCs) such as anomalous file changes and network traffic indicative of malware.



Publish Date: 2024-12-13

Description

Splunk, the data analysis and monitoring platform, is addressing a critical Remote Code Execution (RCE) vulnerability, identified as CVE-2024-53247, which affects several versions of Splunk Enterprise and the Splunk Secure Gateway app on the Splunk Cloud Platform. Rated with a CVSSv3.1 score of 8.8, this vulnerability poses a significant risk to organizations using these services.

3. Data Recovery

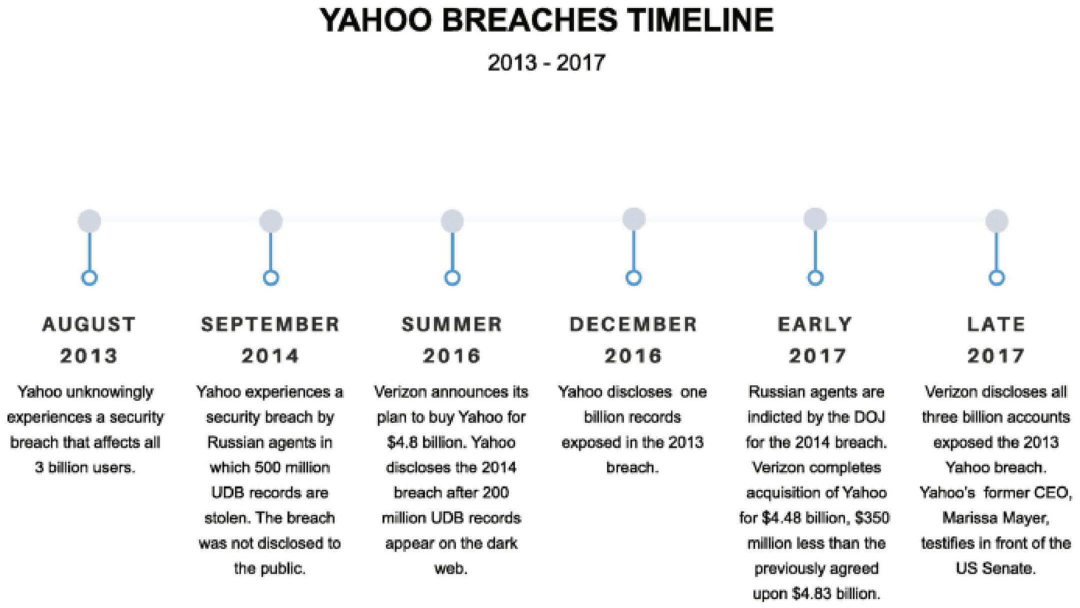
Exposed Data:

- The breach involved the compromise of:
  - 3 billion accounts worldwide.
  - Highly sensitive customer data, including security questions and answers.

Containment and Mitigation:

- Yahoo invalidated unencrypted security questions and answers to prevent misuse.
- Users were prompted to reset passwords and implement two-factor authentication (2FA).
- Temporary account access suspensions were implemented for high-risk accounts.

A detailed timeline of incidents, response and recovery.



YAHOO BREACHES TIMELINE

2013 - 2017

AUGUST 2013

Yahoo unknowingly experiences a security breach that affects all 3 billion users.

SEPTEMBER 2014

Yahoo experiences a security breach by Russian agents in which 500 million UDB records are stolen. The breach was not disclosed to the public.

SUMMER 2016

Verizon announces its plan to buy Yahoo for $4.8 billion. Yahoo discloses the 2014 breach after 200 million UDB records appear on the dark web.

DECEMBER 2016

Yahoo discloses one billion records exposed in the 2013 breach.

EARLY 2017

Russian agents are indicted by the DOJ for the 2014 breach. Verizon completes acquisition of Yahoo for $4.48 billion, $350 million less than the previously agreed upon $4.83 billion.

LATE 2017

Verizon discloses all three billion accounts exposed the 2013 Yahoo breach. Yahoo's former CEO, Marissa Mayer, testifies in front of the US Senate.

Recovery Strategy:

- Yahoo invested in security upgrades, including transitioning to bcrypt for password hashing.
- Enhanced intrusion detection systems were deployed to prevent further breaches.

---

4. Regulatory Compliance:

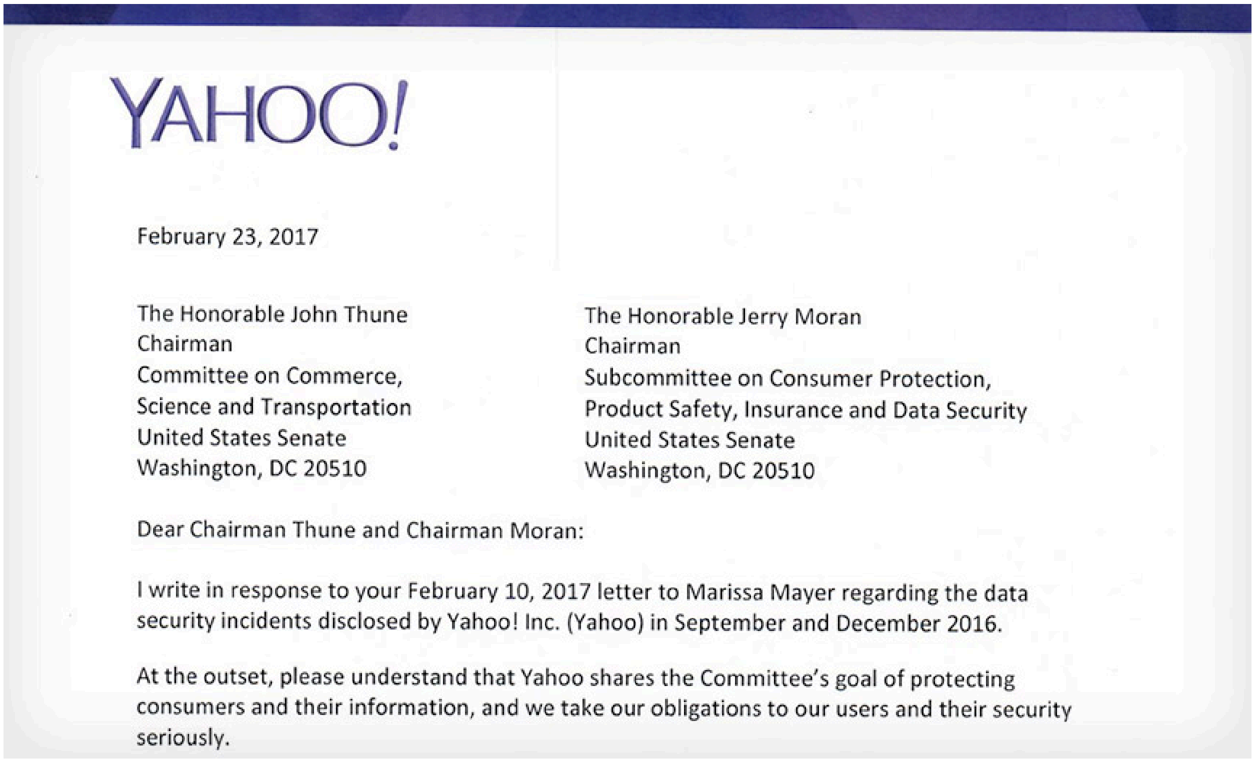
Legal and Regulatory Aspects:

- Yahoo's delayed disclosure of the breach led to regulatory scrutiny.
- In 2018, the U.S. Securities and Exchange Commission (SEC) fined Yahoo $35 million for failing to disclose the breach promptly to investors.
- The breach also triggered class-action lawsuits, culminating in a $117.5 million settlement to compensate affected users.

Reporting:

- Notifications were eventually sent to affected users in 2016 and 2017.
- Yahoo worked with law enforcement and regulatory authorities during its investigation.

A letter and legal report was submitted to the Chairman at that time.



YAHOO!

February 23, 2017

The Honorable John Thune
Chairman
Committee on Commerce,
Science and Transportation
United States Senate
Washington, DC 20510

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance and Data Security
United States Senate
Washington, DC 20510

Dear Chairman Thune and Chairman Moran:

I write in response to your February 10, 2017 letter to Marissa Mayer regarding the data security incidents disclosed by Yahoo! Inc. (Yahoo) in September and December 2016.

At the outset, please understand that Yahoo shares the Committee's goal of protecting consumers and their information, and we take our obligations to our users and their security seriously.

5. Communication and Notification:

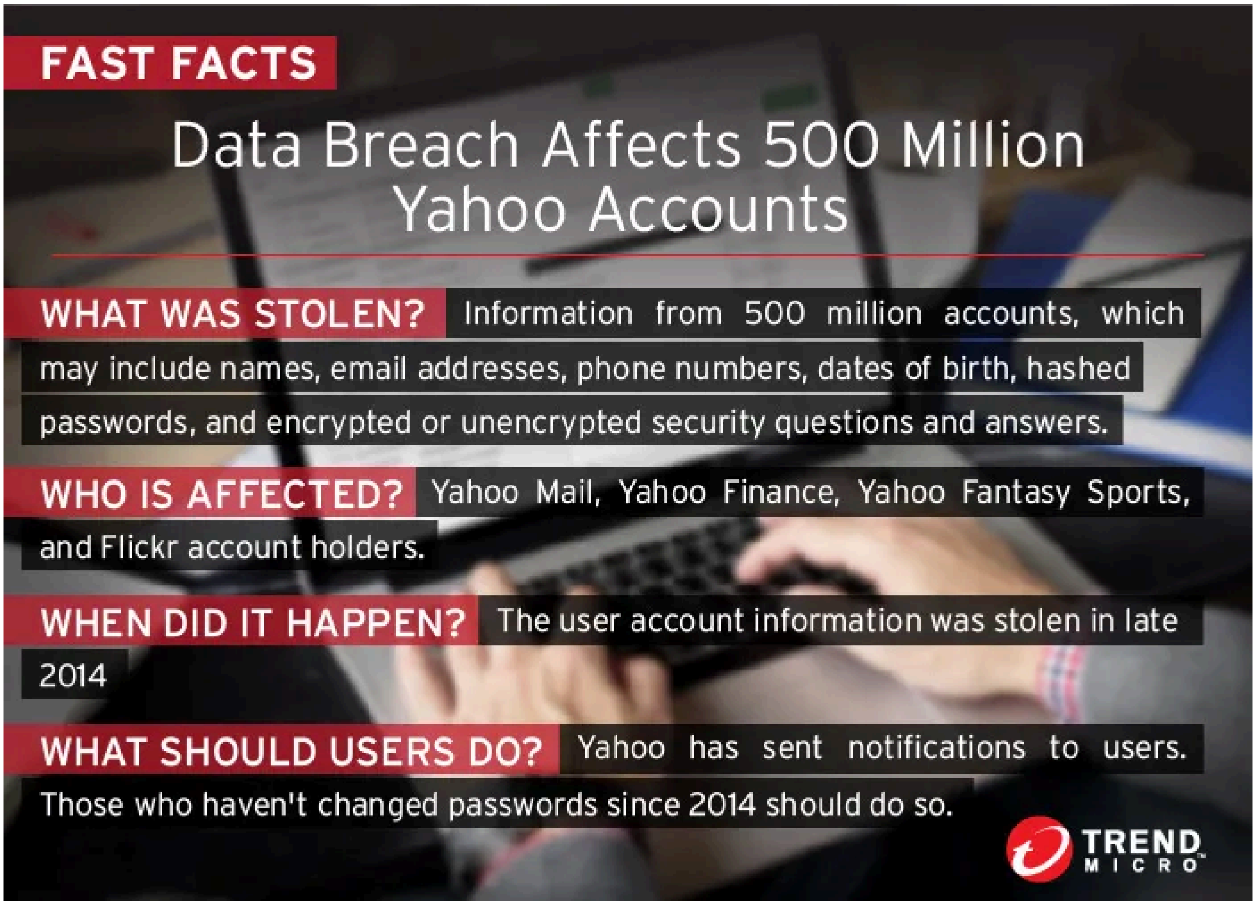
Customer Communication:

- Affected users were notified via email and prompted to update passwords and enable 2FA.
- Yahoo advised users to monitor accounts for suspicious activities and provided security tips to minimize risks.
- Transparency in communication was criticized due to the delay in notifying users and stakeholders.

Stakeholder Management:

- Yahoo’s failure to disclose the breach promptly impacted its reputation and its valuation during the Verizon acquisition.
- Communication efforts post-disclosure included public statements and press releases to manage media narratives.

A brief idea of the list of companies and corporations under Yahoo and its effects from the breach!



FAST FACTS

Data Breach Affects 500 Million Yahoo Accounts

WHAT WAS STOLEN? Information from 500 million accounts, which may include names, email addresses, phone numbers, dates of birth, hashed passwords, and encrypted or unencrypted security questions and answers.

WHO IS AFFECTED? Yahoo Mail, Yahoo Finance, Yahoo Fantasy Sports, and Flickr account holders.

WHEN DID IT HAPPEN? The user account information was stolen in late 2014

WHAT SHOULD USERS DO? Yahoo has sent notifications to users. Those who haven't changed passwords since 2014 should do so.

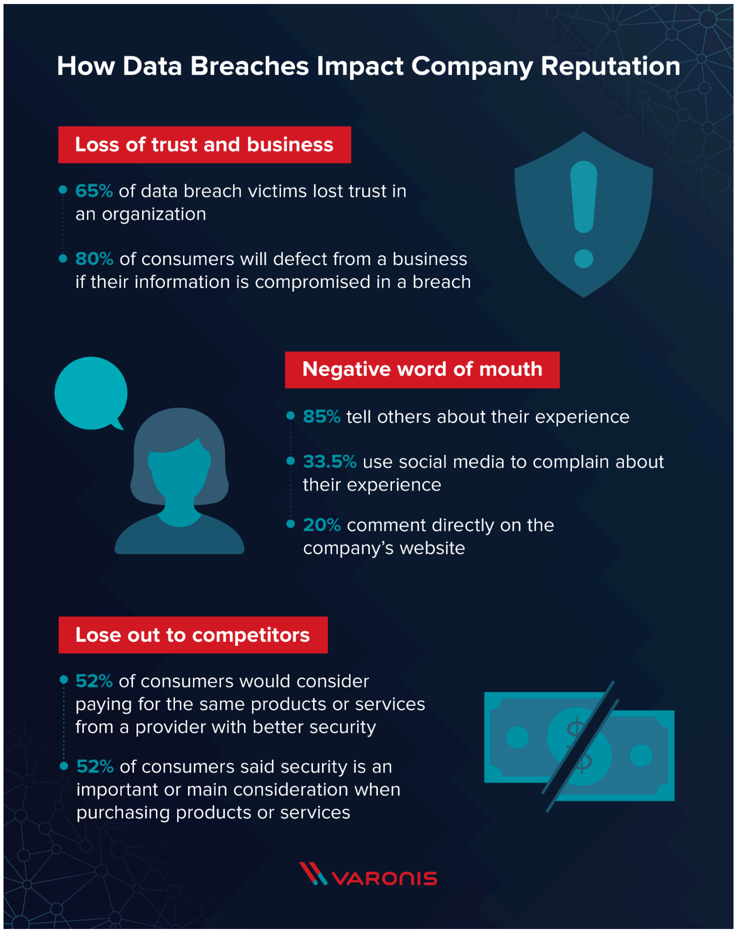
<u>6. Post-Incident Review:</u>

Root Cause Analysis (RCA):

- Outdated security protocols and weak password hashing mechanisms (MD5).
- Insufficient intrusion detection capabilities.
- Poor network segmentation allowed attackers to move laterally within systems.

Lesson Learned:

The major reference and reaction timeline will be observed as;



How Data Breaches Impact Company Reputation

Loss of trust and business

- 65% of data breach victims lost trust in an organization
- 80% of consumers will defect from a business if their information is compromised in a breach

Negative word of mouth

- 85% tell others about their experience
- 33.5% use social media to complain about their experience
- 20% comment directly on the company's website

Lose out to competitors

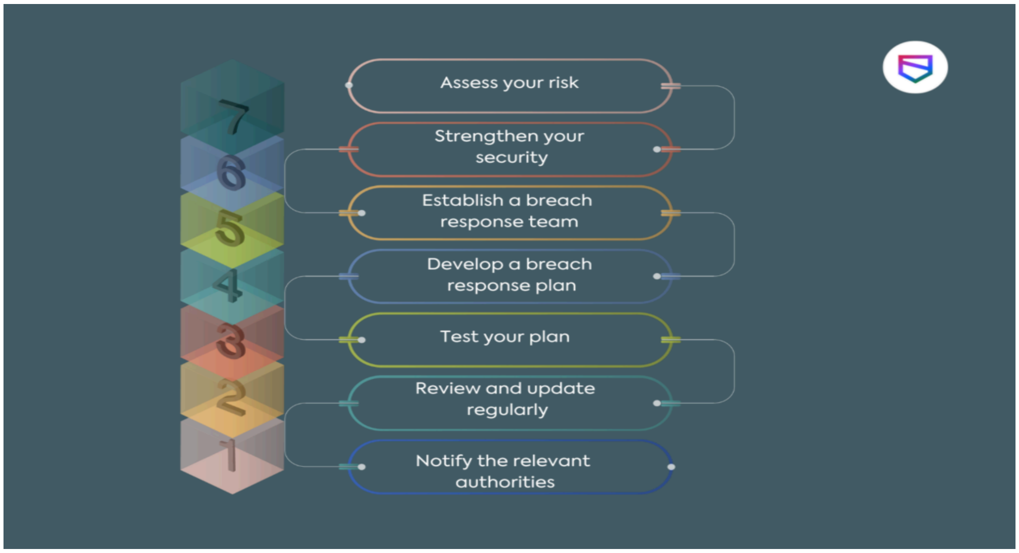
- 52% of consumers would consider paying for the same products or services from a provider with better security
- 52% of consumers said security is an important or main consideration when purchasing products or services

- **Proactive Security Measures:** Regularly update encryption standards and apply patches promptly.
- **Robust Incident Response:** Improve breach detection capabilities and establish clear response protocols.
- **Enhanced User Protection:** Implement stronger account security measures such as mandatory 2FA.
- **Transparency:** Prompt disclosure is critical to maintaining user trust and regulatory compliance.

Recommendations:

1. Transition to industry-standard encryption for sensitive data.
2. Conduct frequent penetration testing and security audits.
3. Provide cybersecurity training to employees to mitigate phishing risks.
4. Implement behavioral analytics to detect anomalies in user activity.
5. Establish a dedicated cybersecurity response team to handle incidents promptly.

A detailed method to avoid "data breaches" at an organizational level!


7
6
5
4
3
2
1
Assess your risk
Strengthen your security
Establish a breach response team
Develop a breach response plan
Test your plan
Review and update regularly
Notify the relevant authorities

Conclusion:

The Yahoo 2013 data breach was one of the largest in history and serves as a major lesson in cybersecurity. Over three billion accounts were compromised, exposing sensitive user data like names, email addresses, and hashed passwords. This incident highlighted significant gaps in Yahoo's security measures, including outdated encryption protocols and inadequate detection systems. Delays in disclosing the breach damaged user trust and the company's reputation.

This breach emphasizes the importance of:

- Maintaining strong cybersecurity defenses by regularly updating and auditing systems.
- Promptly addressing vulnerabilities to prevent exploitation.
- Acting transparently with users and stakeholders during incidents.

Industries worldwide should take this case as a wake-up call to continuously improve security practices and ensure robust measures are in place to protect sensitive data.