Yahoo Break-in

Date: 2024-11-11

Handler: Chao Tang

Executive Summary

In June 2017, Verizon's Security Team found that Yahoo had not fully investigated a 2013 data breach before acquisition. Verizon's assessment revealed that Yahoo had been slow to identify the extent of the breach, which affected all accounts. This delay in detection exceeded industry standards for incident response, leading to incomplete information before the acquisition deal closed. As a result, Verizon faced unexpected costs related to additional security measures and user protections. The total financial impact to Verizon was estimated at $350 million.

Background

In what is considered the largest data breach in history, all 3 billion Yahoo user accounts were compromised by a 2013 breach that went undetected for three years. The attackers, believed to be state-sponsored hackers from Russia, stole names, email addresses, phone numbers, birthdates, and encrypted passwords from Yahoo's user database. A separate 2014 intrusion also allowed hackers to gain the account keys needed to access the private information of over 500 million accounts. The massive Yahoo breach highlighted the vast amounts of sensitive user data that tech firms have access to and their vulnerability to sophisticated cyber attacks.

The intruders also obtained the security questions and backup email addresses used to reset lost passwords — valuable information for someone trying to break into other accounts owned by the same user, and particularly useful to a hacker seeking to break into government computers around the world. Because many of the three billion Yahoo

accounts belonged to people who use the same passwords for different sites and services, there was likely to be an escalation of email fraud and account takeovers. Digital thieves made off with the stolen user account information, including names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicated that the information that was stolen did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information were not stored in the system the company believes was affected. With the stolen data, fraudsters had a higher chance of gaining access to the victims' bank accounts, since most people reused passwords or made multiple versions of the same passwords that were easy to hack.

And there was no timely intervention from Yahoo to mitigate its security measurement breach, which was induced by the fear of incurrence of significant legal and financial exposure, and the possibility of slumping user satisfactions. Yahoo hesitated in enacting the basic remedy to force password reset. It is terrified that even something as simple as a password change would drive its shrinking email users to other alternative services. It was until 2017, after being acquired by Verizon Communications, Yahoo's data breach was finally resourcefully investigated by forensic experts and cybersecurity analysts, and a correct formal disclosure was made to the public.

Timeline

2013-08 — The first data breach occurred on Yahoo servers and affected all three billion user accounts.

2014-11 — A hacker copied a backup of Yahoo's User Account Database, containing details of over 500 million accounts to a computer under his control.

2016-06 — Account names and passwords for about 200 million Yahoo accounts were presented for sale on the darknet market site TheRealDeal.

2016-09-22 — Yahoo officially reported the 2014 breach to the public.

2016-12-14 — Yahoo announced the August 2013 data breach, and disclosed that one billion users have been compromised.

2017-03 — The Department of Justice charged four men, including two Russian intelligence officers, with the 2014 breach.

2017-10 — Verizon Communications, which acquired Yahoo this year, assisted Yahoo to revise the estimate that all three billion users have been affected in the August 2013 breach.

Findings

Paid criminal hackers collected information through computer intrusions in the U.S. and elsewhere and obtained access to the email accounts of thousands of individuals. In or around November and December 2014, they stole a copy of at least a portion of Yahoo's User Database (UDB), a Yahoo trade secret that contained, among other data, subscriber information including users' names, recovery email accounts, phone numbers and certain information required to manually create, or "mint," account authentication web browser "cookies" for more than 500 million Yahoo accounts.

Attackers also obtained unauthorized access on behalf of the Russian FSB conspirators to Yahoo's Account Management Tool (AMT), which was a proprietary means by which Yahoo made and logged changes to user accounts. They then used the stolen UDB copy and AMT access to locate Yahoo email accounts of interest and to mint cookies for those accounts, enabling the co-conspirators to access at least 6,500 such accounts without authorization.

Some victim accounts were of predictable interest to the Russian FSB, a foreign intelligence and law enforcement service, such as personal accounts belonging to Russian journalists; Russian and U.S. government officials; employees of a prominent Russian cybersecurity company; and numerous employees of other providers whose networks the conspirators sought to exploit. However, other personal accounts belonged to employees of commercial entities, such as investment banking firms,

transportation companies, U.S. financial services and private equity firms, bitcoin wallet and banking firms and a U.S. airline.

One of the attackers also exploited his access to steal financial information such as gift card and credit card numbers from webmail accounts; to gain access to more than 30 million accounts whose contacts were then stolen to facilitate a spam campaign; and to earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic.

Actions Taken

Upon discovering the breach, Yahoo took action to contain unauthorized access by invalidating forged cookies used by attackers. These cookies allowed hackers to bypass password requirements and granted direct access to user accounts. Yahoo's technical team responded by disabling and reissuing authentication cookies for all affected accounts. This measure nullified the attackers' ability to exploit the compromised cookies and blocked further unauthorized access through this method. Additionally, Yahoo strengthened its encryption protocols across its systems, upgrading encryption techniques like MD5 to more secure standards for intruder decryption. Yahoo also collaborated closely with law enforcement agencies, including the FBI, to conduct thorough investigations into the breaches. This collaboration aimed to trace the attackers and determine their motives and methods. Yahoo provided law enforcement with relevant data and technical support, which contributed to identifying and prosecuting those responsible.

When Verizon acquired Yahoo in 2017, it took further steps to secure and integrate Yahoo's systems within its own cybersecurity framework. Verizon consolidated Yahoo's internet operations under a new subsidiary called Oath and conducted an in-depth security audit. This assessment identified existing vulnerabilities and provided a roadmap for strengthening Yahoo's security infrastructure. Verizon invested significantly in advanced cybersecurity technologies, including real-time threat detection systems,

enhanced encryption standards, and multi-factor authentication, to protect user accounts and data.

Additionally, Verizon took measures to restore user confidence and address potential fallout from the breaches. They offered credit monitoring and identity protection services to affected users, a proactive step to help users monitor and respond to any suspicious activity tied to their compromised information. Verizon also committed to transparent communication about security improvements, regularly updating users on new security measures and best practices for account protection. These actions were part of a broader effort to rebuild trust, enhance service reliability, and prevent future incidents across the integrated platforms.

Financial Impact

Item	Cost
Regulatory Fines	$35,000,000
Legal Settlements	$117,500,000
Investigative Costs	$25,000,000
Labor Costs	$50,000,000
Total	**$227,500,000**

1. Regulatory Fines: Yahoo agreed to pay a $35 million penalty to the U.S. Securities and Exchange Commission (SEC) for failing to disclose the 2014 data breach in a timely manner.

2. Legal Settlements: The company settled a class-action lawsuit for $117.5 million, covering affected users and providing credit monitoring services.
3. Investigative Costs: Yahoo incurred approximately $25 million in expenses related to forensic investigations, security enhancements, and collaboration with law enforcement agencies.
4. Labor Costs: The breaches required extensive internal resources, including IT personnel, legal teams, and customer service representatives. Assuming an average hourly rate of $100 and an estimated 500,000 hours dedicated to breach response and remediation, the labor costs amount to $50 million.

Lessons Learned

Successes

- Implement high-quality firewalls, antivirus, and intrusion detection systems to monitor traffic and block malicious attacks.
- Use strong encryption and multi-factor authentication to ensure secure access to sensitive systems and data.
- Conduct regular training to educate employees on cybersecurity best practices and reduce risky behaviors.
- Ensure that privacy and security of communications are maintained according to legal standards, emphasizing that unauthorized access will not be tolerated.
- Limit administrator privileges and segment networks to minimize access and reduce potential damage from attacks.
- Conduct regular vulnerability assessments and penetration tests to identify and address potential security weaknesses.
- Understand that without robust cybersecurity measures, companies face increasing costs from data breaches and network disruptions due to emerging digital threats.

Opportunities for Improvement

Issue:

- **Delayed and Incomplete Investigation**: Full investigations were not conducted in a timely manner. Verizon's investigative team was unaware of the full extent of the 2013 breach before acquiring Yahoo, leading to an incomplete understanding of risks. It was surprising to experts that, even after Yahoo discovered one billion accounts were affected, the company did not extend the investigation to consider all user accounts compromised. This delay in identifying the breach (two years) far exceeded industry averages, which, according to the Ponemon Institute, stand at 191 days for discovery and 58 days for containment.
- **Reporting Requirements Not Met**: Yahoo failed to meet industry-standard reporting requirements regarding the breach timeline, leaving Verizon and stakeholders with an incomplete security status.
- **Limited Leadership Access**: Lack of accessible information for leadership restricted their ability to assess the breach's impact, leading to costly aftermath actions and reputational damage.

Recommendation:

- Improve incident response timeliness by establishing a comprehensive investigation protocol to expedite detection and containment within industry-standard timelines. Following an incident, investigations should expand to assess all potential account compromises, especially for large user bases.
- Comply with reporting standards by implementing automated reporting tools that ensure timely updates are provided to stakeholders.
- Enhance leadership briefing procedures by developing streamlined communication channels to keep senior leadership fully informed on security incidents. This can mitigate risks of costly cover-ups and regulatory penalties.

Action Item Owner:

- IT and Security Leadership Team: Responsible for improving investigation protocols and implementing quicker detection and response mechanisms.

- Compliance Department: Ensures that all breach notifications meet industry standards and regulatory requirements.
- Executive Management: Takes charge of updating communication policies to ensure real-time access to incident updates for leadership.