Table of Contents

**Introduction**

Summary of the Incident

Best Preventative practices

**Litigation Exposure**

Conclusion

Information sources

**Introduction**

Jerry Yang and David Filo established the American technology company Yahoo in the first month of 1994. It quickly rose to prominence as one of the early leaders of the internet era by providing a variety of online services, such as a web portal, search engine, email, news, and more. Over the years, Yahoo experienced significant growth and became one of the leading internet companies, attracting millions of users worldwide. It went through various phases of expansion and diversification, acquiring several other companies and launching new products and services. The security of Yahoo's users' accounts was jeopardised in 2013 when a significant data breach occurred. The company revealed that roughly 3 billion user accounts had been impacted by this breach in September 2016. Usernames, email addresses, passwords, and security questions and answers were among the information that was stolen. The hackers also got their hands on the backup email addresses and security questions that were used to reset lost passwords. These pieces of information are crucial for anyone attempting to break into other accounts belonging to the same user and are especially helpful to hackers attempting to hack into government computers around the world.

In June, Verizon purchased Yahoo for $4.48 billion. The disclosure of the breaches, however, almost put an end to the agreement, and Verizon's initial offer was reduced by $350 million. Oath, a new division of the telecommunications company, was created by combining Yahoo with AOL, another fading web pioneer that Verizon purchased in 2015. It surprised outside cybersecurity analysts that investigators did not determine the full scope of the 2013 incident before Verizon finalised the acquisition of Yahoo in June. After the breaches were made public, Yahoo was the target of several shareholder lawsuits, and Verizon may now face greater financial obligations as a result of the revelation that data on all of its accounts was stolen.

**Summary of the incident**

Yahoo's security breaches were caused by sophisticated, state-sponsored cyberattacks that are thought to have been carried out by foreign hackers. To gain unauthorized access to user data, the attackers employed a variety of techniques, including exploiting holes in Yahoo's network and systems. Among the stolen information are names, email addresses, phone numbers, dates of birth, and encrypted passwords, but not credit card information. Yahoo has twice updated its disclosure of a data breach since September 2016. In December 2016, Yahoo revealed that criminals stole data from 1 billion Yahoo users in August 2013 and had also created fake cookies in 2015 and 2016 that would have allowed an intrusive to access user accounts without providing a valid password. On March 1, 2017, Yahoo submitted its 2016 Form 10-K, stating that a state-sponsored actor was responsible for the hacking incident in 2014 and that an unauthorized third party was responsible for the hacking incident in August 2013. Yahoo said about the occurrence from August 2013 that they were not able to determine the hacking activity linked with that theft.

The attorney general for Yahoo resigned on the same day that an independent committee of the Yahoo Board received an internal investigation report that claimed that the 2014 Security Incident was not properly investigated and examined at that point, and the organization was not properly suggested regarding the legal and commercial hazards connected with the 2014 Safety Incident. According to the results of the internal investigation, senior executives and pertinent legal staff were informed in late 2014 that a sponsored by the state actor had gained access to some user accounts by abusing the business's account leadership tool.

A federal judge in California partially rejected Yahoo's motion to dismiss the class action lawsuits related to the data breach on September 1. Then, on October 3, 2017, Yahoo revealed that the hacking activity that dates to August 2013 had probably affected all its users of 3 billion accounts. An attorney for Yahoo claimed that the company had confirmed the updated totals on October 2, 2017, based on additional forensic analysis completed in September 2017, during a subsequent hearing in the consumer data breach class action. According to Yahoo's counsel, recent information about the size of the August 2013 breach that was obtained from a third party served as the impetus for that forensic investigation. The federal judge granted the plaintiffs' request to amend due to the new disclosures. The MD&A (Management's Discussion and Analysis) of Yahoo's financial condition and operating results was also deceptive because it left out well-known trends and unknowns regarding liquidity or net revenue as they were affected by the 2014 breach. Yahoo nevertheless submitted a July 2016 proxy statement regarding its suggested sale to Verizon Communications that erroneously denied being aware of any such significant breach despite knowing full well about the breach. Additionally, it submitted an investment consensus that, as far as it was aware, materially misrepresented the absence of data breaches.

The management and legal teams at Yahoo were notified of the data breach within days of it being found, but they did not properly investigate it and made no attempt to inform investors. According to the SEC's description of the deficiency, Yahoo senior management and the pertinent legal staff failed to adequately evaluate the scope, financial impact, or legal ramifications of the breach, including how and where the breach should have been disclosed in Yahoo's public filings and whether the fact of the breach made any statements Yahoo made in those filings misleading or would do so in the future. Additionally, Yahoo's in-house attorneys and management did not provide information to its auditors or outside counsel for the purpose of determining the disclosure requirements in public filings.

Unsurprisingly, one of the four hackers charged with the Yahoo cyberattacks (and the only one in American custody) showed up for sentencing before a U.S. District Judge in San Francisco on the same day the SEC announced its administrative order and fine against Yahoo. An indictment against Karim Baratov, a 23-year-old hacker-for-hire, for various computer hacking, economic espionage, and other offenses connected to the 2014 Yahoo intrusion was made in March 2017. Two FSB officers and a Russian hacker who was placed on the FBI's list of Cyber Most Wanted since November 2013 are his co-defendants who are still in Russia. The indictment claims that Russian intelligence agents carried out the hacks on Yahoo's systems using criminal hackers, and that they later used some of the stolen data to gain access to other accounts belonging to the targets.

**Best Preventative Practices**

1. **Setting Up Sharing Rules for Classified Information**

Important information should be protected in all forms of communication, and leadership and staff members of an organisation need to understand this. Email is still the primary method of business communication, but to protect sensitive information within an organization's IT infrastructure, appropriate security measures must be put in place. Compliance and policy managers should have policies and procedures outlining how federal regulators, such as the SEC, expect organisations to protect sensitive information from hackers and other cyber-attacks in place.

1. **Preserving information disclosure guidelines**

Organisations are under pressure from federal regulators like the SEC and FCPA to disclose specific information when breaches or other similar events occur. The cyberattacks Yahoo experienced, for instance, started in 2014 but weren't immediately reported to the appropriate authorities. If violated, federal security laws have serious compliance repercussions. If businesses fail to properly disclose crucial security procedures, they risk receiving significant fines and legal action. Even though many organisations already have disclosure protocols in place, compliance and policy managers still need to be aware of the constantly evolving laws they must follow and the policies they must implement to comply with them.

1. **Keeping Information and Documents Secure Away from Emails**

Important documents should not be stored in emails, especially if a company uses service providers outside of its firewall. Emails are too insecure for this. If a user account is compromised, malware and other cyber-threats may get inside the company, which raises a whole new set of issues for compliance managers. Many businesses are aware that using policy management software and contract management software is essential for securely storing documents, contracts, and sensitive information. With Converge Point’s compliance management solutions integrated into a company's SharePoint ecosystem, confidential data is kept in one place rather than travelling through unsafe email channels.

1. **Continuous Monitoring and Logging**

Implement reliable security monitoring and logging solutions to continuously monitor and log system and network activity. Log analysis can assist in spotting unusual or suspicious behavior that might point to a breach.

**Strategies/Policies to be Initiated Once the Incident Has been Detected:**

* Switch on the incident response system
* Security Team Involvement
* Notify the authorities and management.
* Containment and Eradication
* Notify Affected Parties
* Data Restoration

**The company should take the following actions to recover from the incident:**

* Confirm the breach occurred but be wary of emails.
* Determine what sensitive information was taken and made available to hackers. Protect your logins, passwords, and PINS by adding 2FA or MFA.12.
* Change the passwords on any accounts that could be affected, especially those that deal with financial data, and notify your bank of any potential fraud by checking your statements for unusual charges.
* Pay particular attention to government, financial, and healthcare breaches1.
* To stop further data loss, immediately mobilize your breach response team.
* Engage a forensic expert to locate, save, and examine electronic equipment and data to determine exactly what transpired. Disconnect affected communications and isolate compromised systems.

**The Incident Responses:**

* Particularly for securities law purposes, known incidents that could be considered material must be considered in SEC disclosures. When a company has actual knowledge of significant cyber incidents, speaking in the future tense about potential incidents won't be sufficient anymore.
* Lawyers' jobs may be on the line if they don't play a significant part in the investigation and response to cyber incidents. Investigations into cyber incidents are some of the most difficult ones there are. Dabblers and novices should avoid this area. In-house attorneys with real experience and knowledge in cybersecurity and cyber incident investigations are needed by organisations.
* The crisis of cyber incident response requires senior executives to develop their skills. Before they were publicly disclosed, Yahoo's senior executives were aware of the breaches.

**Litigation Exposure**

1. An important cybersecurity breach may result in brand value loss for the company, customer churn, reduced revenue, and other reputational consequences.
2. Compared to class actions for consumer data breaches, securities fraud class actions may fare much better. A strong securities class action that resulted in a settlement of $80 million was sparked by the significant stock decline and blatant misrepresentations regarding the important fact of a significant data breach. Plaintiffs in securities fraud cases do not have a problem with there being any financial loss to customers whose accounts were compromised.
3. The discovery phase will more frequently be reached in class actions involving consumer data breaches. The time of early terminations due to lack of standing is quickly passing. Due to this change, each step of the response process and proper internal investigation into incidents will become much more crucial.
4. The data is trending very favorably for victims, even though it is still unclear how any specific federal judge will sentence a specific hacker. Hacks that target the exploitation of personal information, at least at the federal level, are frequently met with harsh penalties. The best chance a hacker has is to cooperate extensively and receive government-sponsored sentencing reductions. This pattern should encourage both organizations and individual hacking victims to report these crimes to federal law enforcement and to assist in the investigation and prosecution of the cyber criminals who target them.
5. The DOJ's willingness to fight hard for a severe sentence in cases like this one sends a strong message to the private sector that victims will be taken seriously and protected if they cooperate with the law enforcement community to combat serious cybercrime activity, even if a particular judge ultimately rules against the government's requested hacking sentence.
6. Even if the breach happened outside of an organization's own network, it could still result in legal action if the breach came from the system of a third-party vendor or contractor.
7. Failure to uphold contractual obligations could result in claims for breach of contract if the company had contracts with clients, partners, or suppliers that stipulated cybersecurity standards.
8. For potential legal actions, properly preserving evidence connected to the breach is essential. Spoliation claims may result from failing to preserve evidence, which would be detrimental to the organization's defence.

**Conclusion**

Anything we've learned from the Yahoo data breach is that no company is safe from attack. In a 2014 attack, at least 500 million user accounts were compromised, according to Yahoo. Users' names, email addresses, phone numbers, dates of birth, and encrypted passwords were among the stolen data. For the security of customer information, data encryption is essential. While passwords are encrypted by major companies like Google, Facebook, and Yahoo, other sensitive information like date of birth is frequently left unencrypted due to business considerations. For their business models, advertising companies might prioritize having easy access to such data. The more data that businesses choose to encrypt, though, the more protected their customers' data will be from potential hacks and online threats. By strengthening user account resilience and making it more difficult for cybercriminals to breach the main vault, multi-factor authentication is a potent deterrent against thieves.

It is crucial to use defense in depth. Organizations must adopt multiple layers of security across their entire network in addition to encryption and cutting-edge authentication techniques. In-depth penetration testing is essential to find and fix vulnerabilities because, despite ongoing discussions, data breaches are still on the rise. The importance of ongoing user and employee education on security best practices cannot be overstated. In addition, it's essential to have a prepared response strategy in case of a breach to manage and lessen the impact of cybersecurity incidents. As attackers can still get past solid defenses, businesses must operate under the assumption that they will be compromised. Businesses need a clear action plan, clearly defined roles and responsibilities, and effective communication management to be ready for such scenarios. Rapid and effective responses to cybersecurity incidents may result from proactive breach response planning.

**Information Sources**

1. Wikipedia contributors. (2023b). History of Yahoo! Wikipedia. <https://en.wikipedia.org/wiki/History_of_Yahoo>!
2. Perlroth, N. (2017, October 3). All 3 billion Yahoo accounts were affected by 2013 attack. The New York Times. <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>
3. BBC News. (2016, September 23). Yahoo “state” hackers stole data from 500 million users. BBC News. <https://www.bbc.com/news/world-us-canada-37447016>
4. The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far). (n.d.). The National Law Review. <https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far>
5. Yahoo’s Data Breach – 3 Must-Have Compliance and Policy Management Processes – SharePoint Compliance Management Software. (n.d.). <https://www.convergepoint.com/policy-management-software/yahoos-data-breach-3-must-have-compliance-and-policy-management-processes>
6. Pkware. (2022). The Yahoo Breach: Four lessons. PKWARE®. https://www.pkware.com/blog/the-yahoo-breach-four-lessons