ASA

Annie Searle & Associates LLC

Research Note

Privacy and Security: The Largest Data Breach in the History of the Internet

Dominik Żmuda

July 2017

Keywords: Data Security;

Abstract: This paper discusses the risks and fallout associated with Yahoo announcing in September 2016 that in late 2014, data associated with more than 500 million user accounts had been stolen. Virtually all possible events associated with risk exposure arose from the biggest data breach in the history of the Internet.

Privacy and security are always the top-most concerns when dealing with and handling sensitive personal information, including personally identifiable information (PII) and personal user data. All organizations, enterprises, and companies establish their own methods of data security and protection within a certain context and most often, different types of data are handled differently - purely based on the risk associated if that data should be lost or mishandled. As defined by the International Organization for Standardization (ISO), risk is "the effect of uncertainty on objectives,"[1] whereby it is possible to gain or lose something of value based on wagering something else (i.e. risking your life to save your drowning dog).

We have witnessed many events throughout the lifetime of the Internet whereby data had been accidentally lost, leaked, or hacked as a result of potential internal control failures within the governing organization or enterprise of that specific data. While many different types of risk exist within each organization (strategic, compliance, financial, reputational, etc.), operational risk is the highest at stake when dealing with the nature of privacy and security. Internal failures are a direct cause of operational risk within the company's people, process, systems, or even external events (a third-party breaching data, for example).[2]

The year of 2016 will arguably be remembered as the year of discovery within the technological

sector. New technologies have emerged, obsolete systems were rediscovered, and privacy and security has tremendously increased because of surrounding events (the most famous being the Federal Bureau of Investigation vs. Apple, Inc. dispute whereby the FBI put pressure on Apple to hack a terrorist's iPhone).[3] While privacy and security have tremendously increased, we cannot apply this principle to all contexts - this year alone we have discovered many enterprises' services and products we all use, know, and love have been breached with the potential of our personal information being at risk.[4] In 2016, we witnessed the announcements of some of the largest data breaches in history, including the U.S. Department of Justice, the Internal Revenue Service, LinkedIn, MySpace, Dropbox, and the biggest of them all, Yahoo.

In September 2016, Yahoo, one of the biggest online search engines, announced that in late 2014, data associated with more than 500 million user accounts had been stolen (over half of all active accounts).[5] This breach amounts to be the biggest in the history of the Internet, bigger than the LinkedIn and MySpace breaches combined. The company claims the breach was not previously discovered and is "state-sponsored," though has not disclosed which country is responsible. Stolen data includes names, email addresses, telephone numbers, security questions and answers, dates of birth, and encrypted passwords.[6] Living and working in a safe and secure online environment in this day and age is necessary - and many believe total security and privacy exist online and all of our personal information and data is protected. It is not - it is vulnerable to anyone and everyone, and if they desperately need the information, they will find a way - they always have.

Yahoo's data breach is the most significant in the history of the Internet as it is the biggest breach having taken place during the lifespan of the entire Internet with 500 million user-related accounts stolen; 200 million of that information has been posted on the dark web for sale.[7] While the company claims the attack was carried out by a "state-sponsored actor," it has not mentioned what state might be involved; speculations rose around Russia or China. After the announcement of the breach, nearly two years later, most (if not all) Yahoo users and customers were furious the breach hadn't been announced earlier, though Yahoo claims it had no insight before August of 2016, when it acknowledged a potential hack.

Yahoo's breach presents exposure of several different types of risk stemming from the event, not only to the users and company itself, but also to the entire technological world. Due to negligence, Yahoo has essentially placed millions of users at risk of personal information loss or theft as a direct result of the hack. The risk exposure associated with this event is massive, and possesses potential losses to various aspects of the enterprise including user loyalty, operational losses, financial losses, and liability exposure.[8] Fallout included customers who stopped using Yahoo services and products, users filing lawsuits (23 so far) against the company, and Yahoo's brand image being depleted and no longer trusted.

Virtually all possible events associated with risk exposure arose from the biggest data breach in the history of the Internet - Yahoo has now become a brand in which people cannot trust. The sole fact that Yahoo delayed the announcement of the data breach for over two years is a major

issue as users and customers need to be notified immediately in the case of data breach, that way they are able to update their personal information on other accounts or services that may have been linked to their Yahoo account. Although Yahoo claims it had not known of the breach until a few weeks before the public announcement in September of 2016, Fortune, a leading news source, claims "some employees at Yahoo were aware of a recently disclosed major hacking incident when it occurred in 2014."[9] The same article further mentions the company paid more than $1 million to set up an internal investigation committee to research and possibly mitigate the breach before the public could be notified. Yahoo's Chief Executive Officer, Marissa Mayer, was fully aware of the event but "withheld the information from investors, regulators and acquirer Verizon until September."[10] Several sources including the *BBC*, *CNET*, and *The New York Times* claim that Yahoo had knowledge about the event after it occurred and did not announce it to the public until two years later - betraying all users of their services and the general public.

Yahoo knew the breach was major: millions of names, passwords, phone numbers, email addresses, etc. - data pertaining to 500 million user accounts. Investigators and the public began to speculate and try to understand why Yahoo took more than two years to announce the breach. The most plausible reason may be the fact that Verizon was in the process of acquiring Yahoo and their respective services for $4.83 billion[11] - a deal which just closed in 2016. Furthermore, Verizon states that not only did they find out two days before the public, they also have no more information about the breach than what is available to everyone.[12] Marissa Mayer was clearly trying to hide the fact that her enterprise was breached, as the news could have diminished Yahoo's relationship and ended the deal with Verizon. Furthermore, various sources have reported that during the past two years there were "frequent changes in leadership of [the] security team [at Yahoo]."[13] It is a possibility the security team could not handle the large breach or was simply unprepared with no disaster recovery planning in place, and therefore before the public announcement, Yahoo needed to internally "cleanup" and restructure. We can come to a conclusion that Yahoo was clearly trying to hide the breach to those outside of the organization as they were not only unprepared to handle such an event, but also because Verizon might have 'pulled the plug' on the acquisition.

This is not the first time a large data breach has been announced years later. In 2016 alone, it was announced that LinkedIn was hacked (165 million credentials stolen) back in 2012 and MySpace (360 million credentials stolen) in 2013.[13] So why does it frequently take years to announce data breaches by enterprises? A few major reasons include internal investigations, verifications of breach, rapid improvement of current breached systems, and of course, potential pending acquisition of the enterprise by another organization. It is, however, very unethical to wait two years to publicly come forward and admit a system was hacked. *The Conversation* has thoroughly analyzed the Yahoo breach and reports, "as a major internet company with an extremely large user base, it's reasonable to expect Yahoo might detect – and disclose – breaches much sooner than other firms."[14] Yahoo's delayed announcement not only cost them millions of user's trust, but also their public image of being a faithful and reliable enterprise. As Benjamin Franklin once

said, "It takes many good deeds to build a good reputation, and only one bad one to lose it."[15]

Yahoo has definitely set a historical moment in the lifetime of the Internet by acknowledging to withstanding the largest hack in the history of the World Wide Web. It is, of course, perfectly reasonable to believe Yahoo maintained the necessary security protocols and procedures and the breach was 'not their fault'. Hazards and vulnerabilities do not only exist in this event or in Yahoo as an enterprise, but rather in the entire technology sector. Data breaches and potential hacking is always possible, even if you have the most secure system in the world; this breach is no exception and therefore the only blame placed on Yahoo should be for them not issuing a timely announcement.

The vulnerability of data theft and of a potential breach is inevitable, no matter how secure a system is. According to Forbes, the top five data breach vulnerabilities include employees, unsecure mobile devices, cloud storage applications, third-party service providers, and malicious attacks.[16] Often times hackers find loopholes in existing systems and exploit those tiny vulnerabilities to breach a system and once they're in, they have access to virtually everything; while a pathway to a system might be tiny, once it is exploited there is potential for total, unauthorized access. The main reason why we see enterprises improve products and release updates is exactly because of this, and it is crucial to understand nothing is one-hundred percent secure and new vulnerabilities are discovered daily – that is why systems need to be updated and issues need to be reported - even if they do not seem like a major deal.

While we do not know exactly how Yahoo's data was breached, we can only assume the hacker was able to break-in through a vulnerability, exploit it, and gain access to the bigger overall system to steal millions of credentials. Yahoo is continuously working with law enforcement to investigate the breach[5] and identify possible loopholes in their system, it could be possible the vulnerabilities have been discovered, but not yet publicly disclosed. In the case of technology and the online, connected network of computers, servers, and other devices, constant risks, hazards, and vulnerabilities will always exist. There will never be a fully hack-proof system and once a device is connected to the Internet, it is vulnerable.[17] Hackers will always find a way, even if it will take months or years to breach a device. Yahoo's data breach event does not possess any new significance, it is yet another event whereby an organization was hacked and data has been stolen; the scale of the breach, however, is significant. Hazards and vulnerabilities will continue to exist as long as devices are connected together, through the Internet, and no one person or organization will ever be foolproof or immune to data breaches.

Yahoo is a global organization, providing services to users worldwide - the most commonly used ones being the search engine and email services. Yahoo being a non-governmental company based in the U.S. means that while it must follow all of the rules and regulations set forth, the government has no more control over the enterprise than they do of other organizations. There are general business practices and standards each organization must follow, however if the organization is not necessarily providing services directly to the U.S. government, the government then does not have much say over how the enterprise conducts business and what

the internal procedures and policies are.

After the largest data breach in the history of the internet, Yahoo has filed a report with the U.S. Securities and Exchange Commission (SEC) stating it did not know about "any incidents of, or third party claims alleging ... unauthorized access."[18] While Yahoo is working with law enforcement to investigate the breach, the government is not able to necessarily force Yahoo to conduct an internal investigation in a certain manner. As best stated by Reuters, Yahoo's breach "has highlighted shortcomings in U.S. rules on when cyber attacks must be revealed and their enforcement."[18] There are currently no government reporting and/or government regulations that could have prevented this event from occurring. The government has limited control about how companies and enterprises secure their data internally and what each enterprise's security standards are. Furthermore, there is only limited regulation regarding data breach disclosure. There, however, is a possibility that just because of the sheer size of the breach, the government will be able to show more power over Yahoo and their investigation. The breach could push the SEC's guidelines to the limits due to a number of factors - including Yahoo's announcement of the breach taking two years, intense public scrutiny, and the sole fact that the breach is the biggest in the history of the Internet.

There are currently no governmental actions or policies that could have changed the outcome of the breach. In addition, the SEC's 2011 rules on disclosure of breaches for public companies are vague and have not called Yahoo to disclose when the company learned about the 2014 breach.[19] Lawyers and politicians are hoping this breach will open the government's eyes and force it to modify the current SEC rules regarding data breach disclosures as "less than 100 of 9,000 public companies have reported a data breach since 2010."[16] The SEC did impose new regulations in 2014 regarding disclosure of cybersecurity events, however they do not apply to public companies, but rather for broker dealers and investment advisers.

The SEC has never taken action against any company for delays or failures of data breach disclosures, it did however initiate two actions regarding insufficient data protection, both of which are still in progress. According to lawyers, the main reason for no strengthened regulations as far as the government is concerned is because data breaches are "difficult to assess" and the gravity of their effect is not always known at the beginning. A proposed legislation by President Obama and the Democratic Party would legally require companies to disclose breaches within thirty days of internal company acknowledgement. The President states "If we don't act, we'll leave our nation and our economy vulnerable,"[20] however there is a problem - there are currently 47 different data breach statutes across the U.S., each of which apply to different states, and it has been a nightmare in the past to find common ground and policy. The "thirty-days notification provision" would require enterprises to quickly disclose breaches, in addition to reporting to the government about a said breach. Beyond the reporting process, the Federal Trade Commission (FTC) would then be empowered to set and enforce "federal data notification and security standards." While this proposed regulation has not yet been successfully approved, hope is shown for the future of bringing together one common law for data breach disclosures.

While there are currently no government reporting or government regulations that could have prevented the Yahoo data breach from occurring, there is hope for the future regarding data breach notifications to the public and the government. Currently, there are no specific laws regarding how a company should maintain their safety, security, and data protection - at least there is hope for a "disclosure of data breaches" law that would force companies to quickly report breaches. Data breaches affect users the most, as their personal information is then vulnerable to anyone and is at risk of a variety of factors including identity theft. It is of key importance that a law be regulated to force enterprises to disclose breaches in a timely manner for the safety and security of the company itself, the government, and most importantly of all, the loyal users.

The Yahoo data breach is arguably the most significant event taking place in the entire lifespan of the Internet and World Wide Web. At 500 million pieces of user information being breached, just the astounding size of the event makes it significant alone. It is important to note that Yahoo may not necessarily be at fault of anything (apart from the late announcement of the breach), but could rather be a random victim of a malicious attack. The enterprise still has not acknowledged as to why the announcement of the hack took two years, but it has been proven that internally many employees were well aware of the breach after it happened in 2014. The one, single greatest cause for the delayed announcement was Verizon's pending purchase and acquisition of Yahoo for $4.83 billion, a deal which just closed months ago.

The various risks surrounding the event are astounding: millions of users could be victims of data and identity theft simply because Yahoo took an astonishing amount of time to come forward with the message; had Yahoo disclosed information earlier, users would have been able to update their personal information on all related websites and services to be less vulnerable to the breach. The operational risks arising from this event include failures in the company's people, process, systems, and external events. The breach was an external event, however the operation of the process of disclosing and identifying the breach were internal procedures and policies of Yahoo. Many enterprises and companies should use Yahoo's data breach event as a way to improve their own policies, procedures, and security standards. The single, most recommended, item of key importance is to disclose a breach or hack as soon as the event takes place - this will enable all users to take the necessary precautions and measures to ensure their data and identity is safe. Announcing the breach years later betrays the user's trust and faith in a company because by then, the personal information and data from all of the user's services and websites might be floating around in the hands of malicious hackers. Early disclosure of breaches is better and shows the company has ethics and high standards when it comes to safeguarding their customers and users.

Another key recommendation that should be placed into action to reduce the risk around such an event from reoccurring is to have enterprises implement data breach detection systems. These systems would simply run in the background and if a breach or hack was detected, the said system would be able to preserve all company data and take it offline by disconnecting it from the Internet or hacker, and access would be disabled. In the case of a data breach detection system, all of the servers would essentially go offline - neither the users or hackers would have

access, but data would be preserved and would not be vulnerable. Taking an entire company offline would cost millions of dollars, but would be a more effective way than to have millions of personally identifiable user information breached. This system would essentially preserve an enterprise's public image while ensuring user information is safe.

Yahoo's 2014 data breach will always be remembered in the history of the Internet as one of the most significant events due to the sheer size of data being breached. Many users and customers have lost faith and trust in Yahoo due to the data breach announcement taking more than two years - perhaps not just the enterprise is at fault here, but also the government as no strong laws and regulations currently exist dealing with data breaches. The events surrounding the breach have not only drawn a pathway for the government to create new laws and policies regarding cybersecurity issues, but also for the technology sector to keep innovating through risk[21] and improving the current systems to ensure reliability, safety, security, and data protection measures exist and are constantly improved upon. As set forth by the National Institute of Standards and Technology (NIST), enterprises need to ensure the five Framework Core Functions of Cybersecurity risk mitigation (Identify, Protect, Detect, Respond, and Recover)[22] are continuously and concurrently carried out to ensure maximum safety and protection. Had Yahoo followed these key steps, the entire organization would be better regarded as having taken thorough action in the case of the largest data breach of the Internet. While we will never be one hundred percent safe when dealing with the world wide web and internet, there is hope to become safer and smarter as new vulnerabilities and weaknesses become discovered and new technologies emerge, changing the way we interact with the world.

---

[1] "ISO 31000 - Risk Management." ISO 31000. International Organization for Standardization, n.d. Web. 30 Nov. 2016 <http://www.iso.org/iso/home/standards/iso31000.htm>.

[2] Griffin, Dana. "Types of Business Risk." Types of Business Risk | Chron.com. Chron, n.d. Web. 30 Nov. 2016 <http://smallbusiness.chron.com/types-business-risk-99.html>.

[3] "Breaking Down Apple's IPhone Fight With the U.S. Government." The New York Times, 21 Mar. 2016. Web. 30 Nov. 2016 <http://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html>.

[4] Leary, Judy. "2016 Data Breaches." IdentityForce, n.d. Web. 30 Nov. 2016 <https://www.identityforce.com/blog/2016-data-breaches>.

[5] Fiegerman, Seth. "Yahoo Says 500 Million Accounts Stolen." *CNNMoney*. Cable News Network, 23 Sept. 2016. Web. 01 Dec. 2016 <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/>.

[6] Gallucci, Nicole. "Yahoo Confirms Massive Leak of 500 Million User Accounts." Mashable, 22 Sept. 2016. Web. 30 Nov. 2016 <http://mashable.com/2016/09/22/yahoo-confirms-data-breach>.

[7] Burr, Edmondo. "200 Million Yahoo Accounts Show Up For Sale On Dark Web." *Your News Wire*. N.p., 02 Aug. 2016. Web. 01 Dec. 2016 <http://yournewswire.com/200-million-yahoo-accounts-show-up-for-sale-on-dark-web/>.

[8] Baranoff, Etti, Patrick L. Brockett, and Yehuda Kahane. "Risk Management for Enterprises and Individuals 1."

Scribd. Scribd, n.d. Web. 01 Dec. 2016 <http://catalog.flatworldknowledge.com/bookhub/1?e=baranoff-ch01_s04#baranoff-ch01_s04_s01_t01>.

[9] Hackett, Robert. "Yahoo Knew About the Breach in 2014." *Fortune*. N.p., 09 Nov. 2016. Web. 01 Dec. 2016 <http://fortune.com/2016/11/09/yahoo-hack-data-breach-sec/>.

[10] Murgia, Madhumita, Tim Bradshaw, and David J. Lynch. "Marissa Mayer Knew of Yahoo Breach Probe in July - FT.com." *Financial Times*. N.p., 23 Sept. 2016. Web. 06 Dec. 2016 <http://www.ft.com/cms/s/0%2Fd0d07444-81aa-11e6-bc52-0c7211ef3198.html?ft_site=falcon&desktop=true#axzz4S5JMLWip>.

[11] Alesci, Cristina, Seth Fiegerman, and Charles Riley. "Verizon Is Buying Yahoo for $4.8 Billion." *CNNMoney*. Cable News Network, 25 July 2016. Web. 03 Dec. 2016 <http://money.cnn.com/2016/07/25/technology/yahoo-verizon-deal-sale/>.

[12] Szoldra, Paul. "Yahoo Gave Verizon Only Two Days Notice of the Massive Breach of 500 Million Users." *Business Insider*. Business Insider, 22 Sept. 2016. Web. 04 Dec. 2016 <http://www.businessinsider.com/yahoo-verizon-breach-2016-9>.

[13] Kirk, Jeremy. "MySpace, LinkedIn Data Just a Click Away." *BankInfoSecurity*. N.p., 30 June 2016. Web. 05 Dec. 2016 <http://www.bankinfosecurity.com/myspace-linkedin-data-just-click-away-a-9233>.

[14] Ye, Yanfang. "Why Did Yahoo Take so Long to Disclose Its Massive Security Breach?" *The Conversation*. N.p., 30 Sept. 2016. Web. 05 Dec. 2016 <http://theconversation.com/why-did-yahoo-take-so-long-to-disclose-its-massive-security-breach-66014>.

[15] Eccles, Robert G., Scott C. Newquist, and Roland Schatz. "Reputation and Its Risks." *Harvard Business Review*. N.p., Feb. 2007. Web. 06 Dec. 2016 <https://hbr.org/2007/02/reputation-and-its-risks>.

[16] Basu, Eric. "The Top 5 Data Breach Vulnerabilities." *Forbes*. Forbes Magazine, 05 Nov. 2015. Web. 03 Dec. 2016 <http://www.forbes.com/sites/ericbasu/2015/11/05/the-top-5-data-breach-vulnerabilities>.

[17] Mann, Jason. *The Internet of Things: Opportunities and Applications across Industries*. N.p.: Enterprise Research Service, 2015. PDF.

[18] Volz, Dustin. "Yahoo Hack May Become Test Case for SEC Data Breach Disclosure Rules." *Reuters*. Thomson Reuters, 30 Sept. 2016. Web. 04 Dec. 2016 <http://www.reuters.com/article/us-yahoo-cyber-disclosure-idUSKCN1202MG>.

[19] Pymnts. "Yahoo's Breach Epitaph - SEC To Change Breach Disclosure Rules | PYMNTS.com." *PYMNTS.com*. N.p., 03 Oct. 2016. Web. 04 Dec. 2016 <http://www.pymnts.com/news/security-and-risk/2016/yahoos-breach/>.

[20] Amorosi, Drew. "Obama Wants Federal Data Breach Notification Law." *DatacenterDynamics*. N.p., 03 Feb. 2015. Web. 05 Dec. 2016 <http://www.datacenterdynamics.com/content-tracks/security-risk/obama-wants-federal-data-breach-notification-law/93420.fullarticle>.

[21] "The Art of Managing Innovation Risk | Accenture Outlook." *Accenture Outlook*. N.p., n.d. Web. 06 Dec. 2016 <https://www.accenture.com/us-en/insight-outlook-art-of-managing-innovation-risk>.

[22] *Framework for Improving - Critical Infrastructure Cybersecurity*. N.p.: National Institute of Standards and Technology, 12 Feb. 2014. PDF.