Significant Cybersecurity Incidents Throughout History

Annie Jones

Metropolitan Community College

22SP_INFO_2805_H8A - Network & Security Basics

Eric Baumguarten

May 18, 2023

Significant Cybersecurity Incidents Throughout History

Abstract

Since the advent of technology and its implementation into society, there have been individuals seeking to use it for unethical purposes. This research paper will review some of the most notable hacking events throughout history. A description of those attacks and what negative consequences these events had on individuals and organizations will be examined for a thorough understanding of the impact unethical hacking has on society. Due to these historical events, new regulations and standards of procedure are usually implemented. As security threats continue to evolve, remaining vigilant against potential threats is necessary for cybersecurity.

Significant Cybersecurity Incidents Throughout History

While the invention of technology has improved people's lives in almost every aspect, there have also been individuals seeking to use it for unethical purposes. From the first hacking incident in 1834 where two thieves hacked the French Telegraph system to steal financial market information to the billions of individuals affected by singular hacking incidents such as the Yahoo breach in 2013, the need for protection has always co-occurred with technology ("Cybersecurity History: Hacking & Data Breaches," n.d.-b). As security threats continue to evolve, remaining vigilant against potential threats is necessary for cybersecurity. In order to prevent these incidents, it is necessary to have a thorough understanding of how these attacks were accomplished, the negative consequences of these events on individuals and organizations, and the regulations and standards of procedure implemented as a consequence to certain unethical hacking incidents that have impacted society. This research paper will review some of the most notable hacking events throughout history to illustrate the various methods attackers use to gain access to private information.

Prior to the invention of the World Wide Web, a significant incident involving a computer worm brought many education systems and even some government research sectors to a halt. What became known as the Morris Worm occurred in 1988, named after its creator, Robert Tappan Morris. Because it did not require a software host, this computer worm was able to spread on its own. This worm resulted in serious delays in email, military functions, and resulted in several organizations' attempts to resolve the issue on them through means of wiping systems, disconnecting from networks and other plausible solutions for their problem. While the worm did not damage or destroy any files, the cost of damages quickly reached millions of dollars. A tip from one of Morris' acquaintances led authorities to discover the individual behind

this attack. While Morris claimed this to be an innocent prank that got out of control, it illuminated the serious vulnerabilities computers had, which led to computer intrusion software (*Morris Worm*, 2022).

Another costly incident with more sinister intentions was the Russian bank robbery incident in 1994. Unlike any heist previously committed, this crime took place in St. Petersburg, Russia with its victim being a major US Bank. Upon the discovery of approximately $400,000 being discovered missing from customer accounts, authorities were involved. It was determined the attackers were able to use the telecommunications network to gain access to the bank's cash management system, allowing them to transfer funds outside of the owners' accounts. The FBI was able to calculate losses of over 10 million dollars over a period of 5 months. After pinpoint a couple involved who were attempting to withdraw the stolen money, the FBI was able to work with Russian authorities to track down the man behind what was considered the first online bank robbery, Vladimir Levin. This incident prompted the FBI to begin "expanding its cybercrime capabilities and global footprint, steadily building an arsenal of tools and techniques that help us lead the national effort to investigative high-tech crimes today" (*A Byte Out of History: $10 Million Hack*, 2016).

In 2013 Adobe made national headlines for its lack of data protection of about 38 million active users, including credit card numbers, login information, digital assets, and more. This was made possible by theft of source code for Adobe Acrobat, Reader, ColdFusion, and Photoshop which later appear on AnonNews.org. As a result, Adobe offered users a one year of credit monitoring through Experian (*Adobe Breach Impacted at Least 38 Million Users*, 2013). They

were also required to pay over 1 million dollars in legal fees in addition to undisclosed settlements for violation of the Customer Records Act (Swinhoe, 2022b).

Arguably one of the most significant hacking events in history was the Yahoo breach that occurred in 2013. What was initially estimated at over one billion accounts was revised to an astonishing 3 billion user accounts that were exposed due to this breach 3 years later (Swinhoe, 2022c). In 2017, after many properties had been sold to Verizon, 35 million dollars was paid to settle charges for concealing pertinent information about the attack from consumers (Valinsky, 2019b).

While the Yahoo is considered by many to be the biggest breach in history, one of the most expensive incidents, possibly due to its involvement with American's credit history, was the announcement of Equifax's breach in 2017. Some 150 million citizens had their personal information exposed. User information became exposed through a known security issue within in the account issue reporting, by means of a design flaw in a tool called Apache Struts (Larson, 2017). Equifax eventually agreed to pay up to 700 million dollars to state and federal regulators for their lack of oversight. It also led to a required change in how they handle private data that include annual reviews of security risks and board certifications for Federal Trade Commission compliance (Cavaliere & Fung, 2019).

Even recently, cyber-attacks have left individuals' private information susceptible to exploitation and businesses exposing these customers' information with hefty fines for their lack of protection. In 2018 Marriott informed the public that their guest reservation system had been available to an unauthorized user for almost 5 years. They currently face fines of 124 million

dollars in the UK for failure to protect guests' data that fall under Europe's new regulations of the General Data Protection Regulation (Valinsky, 2019c).

It seems only inevitable that a company involved in cybersecurity would become the target of an attack by hackers. Such an event occurred in 2022 when it was discovered a database was vulnerable to exposure. Security researcher, Volodymyr Diachenko, informed Cognyte of the issue and the company was able to secure it three days later. Due to its rapid response, Cognyte was able to block exposure. These records were collected from previous data incidents and contained more than 5 million records (*Security Magazine*, n.d.).

Cybersecurity is a field that is constantly evolving to protect individuals' sensitive information, government data, organization's private data, and more. The need for cybersecurity has become increasingly important. By having a comprehensive understanding of major hacking incidents throughout history, one can gain an understanding of how these events led to significant impacts on individuals and organizations. Additionally, a thorough understanding can aid in the prevention of future attacks as well as possibly solutions to responses of attacks that may occur. This paper illustrates the evolving nature of attacks, their impact on those affected, and the consequences of insufficient cybersecurity measures organizations must face when a security incident occurs.

Significant Cybersecurity Incidents Throughout History

<div align="center">

Works Cited

</div>

Cybersecurity History: Hacking & Data Breaches. (n.d.-b). *Monroe College*.

https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches

Morris Worm. (2022, October 21). Federal Bureau of Investigation.

https://www.fbi.gov/history/famous-cases/morris-worm

A Byte Out of History: $10 Million Hack. (2016, December 20). Federal Bureau of Investigation.

https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

Adobe Breach Impacted At Least 38 Million Users. (2013, November 10).

https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

Swinhoe, M. H. a. D. (2022b, November 8). *The 15 biggest data breaches of the 21st century*.

CSO Online. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-

the-21st-century.html

Valinsky, J. (2019b, July 30). 7 of the biggest hacks in history. *CNN*.

https://www.cnn.com/2019/07/30/tech/biggest-hacks-in-history/index.html

Significant Cybersecurity Incidents Throughout History

Larson, J. W. a. S. (2017, September 16). *How the Equifax data breach happened: What we know now*. CNNMoney. https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html?iid=EL

Cavaliere, V., & Fung, B. (2019, July 22). Equifax exposed 150 million Americans' personal data. Now it will pay up to $700 million. *CNN*. https://www.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html

Security Magazine. (n.d.). https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021