Peter MacMillan

12/11/2023

What Social Scientists Know About Data Breaches?

Introduction

In today's world, the digital frontier has become the subject of many topics related to the safeguarding of information and how to keep that information secure. However, information will never be 100% secure and this can be seen in the unrelenting number of cyber-attacks and data breaches that have happened in recent years. With all of these attacks, people ask themselves; is it really safe to be on the internet or have internet connected devices? The number of these incidents continues to grow and society as a whole does not seem to have a concrete answer on how to prevent them.

This sheds light on the value of personal information on the dark web and how hackers or leakers use it to profit. How safe is our personal information on the internet? That question cannot be answered realistically since we have not seen results and changes being made in the wake of these cyber-attacks and data breaches. This shows us how vulnerable our security systems really are in comparison to the abilities of the adversaries trying to gain access to this information.

This essay will explore this topic through the use of sources relating to several types of data breaches and the factors that play a role in them. Trusted authors write these articles, and they provide insights about these incidents and how they can affect not just big companies, but also the general public.

What are Data Breaches?

Data breaches are easy enough to explain but are complicated in how they are conducted. Most people define them as an unauthorized access to information systems or databases that have the possibility to lead to information leaks or the selling of that information. These kinds of things are not just aimed at big targets but also unsuspecting individuals.

Data breaches can vary in size, cost (in damages), and complexity. As mentioned above, if individuals are targeted, a breach could be considered small but could have huge monetary losses for that individual. The same could be said about big corporations or entities; the breach could be small with a small monetary loss or a catastrophic event with massive monetary losses. These breaches can be caused by a plethora of things. The list includes things like phone calls, social engineering, and good old hacking methods.

What Do We Know About Data Breaches

The first article I chose begins talking about the cybercrime ecosystem and a few of the many actors that play a role in it. James Martin, a senior lecturer, and Chad Whelan, a professor of Criminology, state that "this ecosystem contains various cyber-criminal groups who increasingly specialize in one particular aspect of online crime and work together to carry out the attacks" (Martin & Whelan, 2023). This shows that these cyber criminals are more likely to conduct attacks together rather than doing them solo. This creates a sense of comradery among these cyber criminals and allows networks to form. A more common type of attack, if its even considered an attack, are data breaches. These attacks can lead to serious financial and reputational damage to an organization. This article asks a question about combatting these things. Martin and Whelan think that companies should change their approach to data and how it should be managed. They say that "data should be treated not simply as an asset that can be freely held and traded in, but also as a liability that needs to be carefully protected" (Martin &

Whelan, 2023). This proposed idea could help maintain the security of information for the time being and allow for updated cybersecurity policies and procedures to be implemented.

The second article talks about the genomics company, 23andMe, and how they experienced a data breach of sorts. An interesting takeaway from the article is that their servers were not the target of the hack, but the individual user accounts were. According to the article, “hackers targeted hundreds of individual user accounts, allegedly those who had repeated passwords” (Cofone, 2023). This is interesting because the hackers were looking for a specific pattern to target rather than the company servers themselves. This type of data breach makes us think about how we comprehend privacy, data security, and the accountability of corporate entities. The scary thing about this breach was that the information that was taken was genetic information. This data describes a person’s genetic makeup and pre-disposition results. This information can also be used to find people/relatives that share a similar genetic composition to you. Intertwined data like this can be considered more valuable to hackers since it can lead to more than one person for them to exploit.

The third article focuses on the difference between ransomware and data breaches. One of the most common types of attacks is ransomware. In these attacks, information is encrypted and held hostage, and the adversary requests a ransom of a certain dollar amount, usually in cryptocurrency, to release the information back. Companies usually try to bargain to lower the amount or downright refuse to pay. If that is the case, the adversaries may leak the information anyway or they may take the adjusted monetary amount and relinquish access back to the individual or company. With a data breach, your information may already be leaked to the dark web or made public. This could include bank account information, social security numbers, or lesser things like phone numbers and email addresses. However, having this information leaked

is still something to be afraid of. This article also outlines steps to take in order to protect yourself and your information from the potential threat of a data breach or leak. Warkentin, an information systems professor, expresses the importance of setting up a multi-factor authentication device or tool for logging into systems. He goes on to mention that unique passwords should be used rather than ones that are easy to remember or often repeated.

The fourth article that I found looks at an approach to protect against future breaches with the use of blockchain technology. This kind of technology has come a long way since its inception. A blockchain is described as a database that manages a constantly growing list of ordered records, which are called blocks. The blocks in this system connected by cryptographic means. This means that each block is given the cryptographic hash of the previous one and any other information that goes along with it. With this in mind, a database like this can be used to store personal health information and "allow each individual consumer to manage their own data and how that data is shared" (Lemieux, 2022). There are a few challenges to this kind of proposal. The most glaring one is that cryptographic keys can be long and complicated, not to mention, easy to forget. A proposal from the research within article was for a hybrid system "that gives consumers control over their health data wallets but allows them to reach out to a service to recover their private keys in the event of loss" (Lemieux, 2022). This approach would allow consumers to maximize the security of their information and still have access to a recovery system.

The final article that I found examines the governmental reaction to all of the breaches that have happened in recent years. This article mentions the Sarbanes-Oxley Act, which requires companies to hire external auditors that report directly to the board of directors about anything and everything. The author of the article, Michael Parent, states that this increase in breaches per

year has caused cybersecurity to reach its Sarbanes-Oxley moment. It is well known that breaches have a certain disregard for where they occur and who they target, whether they be part of the public or private sectors. This article points out that companies respond to these breaches inadequately and should look to other legislation that may amend their approach to these responses. Parent (2022) mentions the GDPR policy that the European Union Parliament accepted in 2018 and how it would levy heavy fines on companies in the event of privacy breaches. If the United States as a whole proposes legislation like this, companies and big businesses would have to take data privacy and security more seriously or have to pay the fines for ignoring it.

Conclusion

In a world where we see ourselves becoming more dependent on technology, information security has become of major importance and should not be overlooked. In the past decade or so, we have seen an exponential increase in data breaches and cyber-attacks. While you or I may not experience one, they are happening all over the world and could affect anyone. Certain technological advancements and ideas are coming forth and could prove to be a solution to potential data breaches. However, these ideas and advancements should be taken with a grain of salt because nothing can ever be 100% secure.

By reading this essay, people may gain an idea of what information security is and the best ways to go about securing information that may be important. Data breaches will unfortunately continue to occur, but we have plenty of tools at our disposal to help prevent and mitigate the damage caused from them.

References

Cofone, I. (2023, October 26). The 23andMe data breach reveals the vulnerabilities of our interconnected data. The Conversation. https://theconversation.com/the-23andme-data-breach-reveals-the-vulnerabilities-of-our-interconnected-data-193615

Lemieux, V. (2022, June 16). How blockchain could prevent future data breaches. The Conversation. https://theconversation.com/how-blockchain-could-prevent-future-data-breaches-130122

Martin, J., & Whelan, C. (2023, March 21). Why are there so many data breaches? A growing industry of criminals is brokering in stolen data. The Conversation. https://theconversation.com/why-are-there-so-many-data-breaches-a-growing-industry-of-criminals-is-brokering-in-stolen-data-193015

Parent, M. (2022, May 16). Growth in data breaches shows need for government regulations. The Conversation. https://theconversation.com/growth-in-data-breaches-shows-need-for-government-regulations-127600

Warkentin, M. (2022, September 13). Ransomware, Data Breach, cyberattack: What do they have to do with your personal information, and how worried should you be?. The Conversation. https://theconversation.com/ransomware-data-breach-cyberattack-what-do-they-have-to-do-with-your-personal-information-and-how-worried-should-you-be-162404