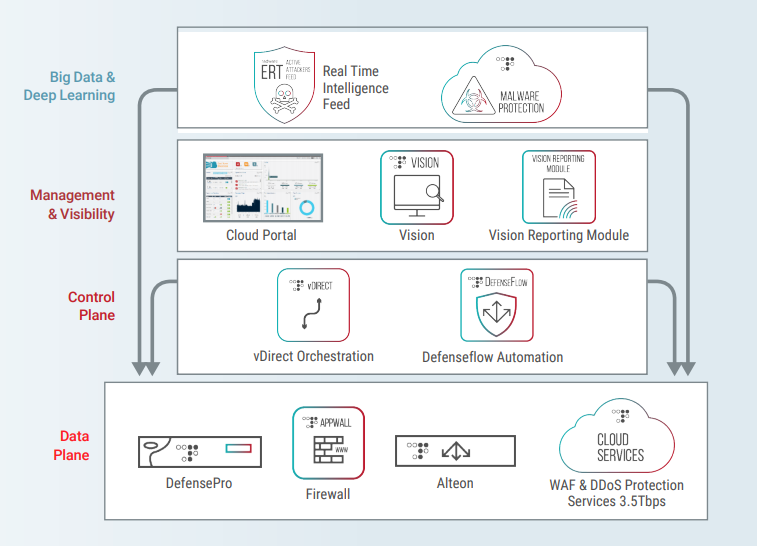
Cyber Attacks on Business’ Cloud Platforms and Big Data



Abstract: Cyber-attacks on big data has become an increasing problem in the technology industry, and measures to reduce the cyber-attacks have become necessary than ever. This paper discusses two ways that businesses can protect their big data on cloud platforms from cyber-attacks. It, however, does not rate the solutions as to which is more accurate in terms of helping companies gain more profits and minimize loss. The research for this paper was obtained from primary and secondary resources.

Key Words: Big Data, Cyber-attacks, Businesses, Profits, Loss

Table of Contents

Contents

[Introduction 2](#_Toc102158394)

[Goals/Objective to combat breach of big data security. 3](#_Toc102158395)

[Protecting Sensitive and Personal Information 4](#_Toc102158396)

[Figure 1: Personal information stolen by hackers 5](#_Toc102158397)

[Lack of Big Skilled Data Security Professionals 5](#_Toc102158398)

[Figure 2: Large Sets of Data Processed by Data Engineers 6](#_Toc102158399)

[Solutions 6](#_Toc102158400)

[Increasing Big Data Security 6](#_Toc102158401)

[Benchmark: Capital One Data Breach 7](#_Toc102158402)

[Avoiding Phishing Attacks and Emails 8](#_Toc102158403)

[Benchmark: Protecting Your Organization from Cyber Attacks 8](#_Toc102158404)

[Assessment 9](#_Toc102158405)

[Table 1 9](#_Toc102158406)

[Works Cited 10](#_Toc102158407)

[Appendix A: Business and Healthcare Breaches 11](#_Toc102158408)

[Appendix B: Data Breaches Over the Years 12](#_Toc102158409)

# Introduction

Big data is important for businesses. Companies use big data to predict their growth and ways they can maximize their profit and gains. Just as big data has opened new possibilities for businesses, it has also given hackers and cyber criminals the chance to steal and access large quantities of sensitive and personal information. Companies can measure the increase in cyber-related crimes against their customers by keeping records of all cyber-attacks. The increasing reliance on big data and cloud platforms also creates a broader scope for hackers to exploit vulnerabilities. The rise in cyber-attacks is concerning for both businesses and individuals. In the United States, the number of cyber-attacks grows by 27% yearly. The top two challenges that businesses face with big data that compels hackers to steal from them are protecting sensitive and personal information and lack of skilled big data security professionals to protect business and customer data.

# Goals/Objective to combat breach of big data security.

* Increase big data security resources in companies by 40% or more by 2025.
* Big data kept 90% confidential by 2025.
* Protect 85% of big data from unauthorized access by 2022.
* Reduce over 85% cyber-attack on big data by 2030.
* Safe internet connection available to industries by 2025.
* Requirement for industries to monitor logs and integrity of big data by 2025.

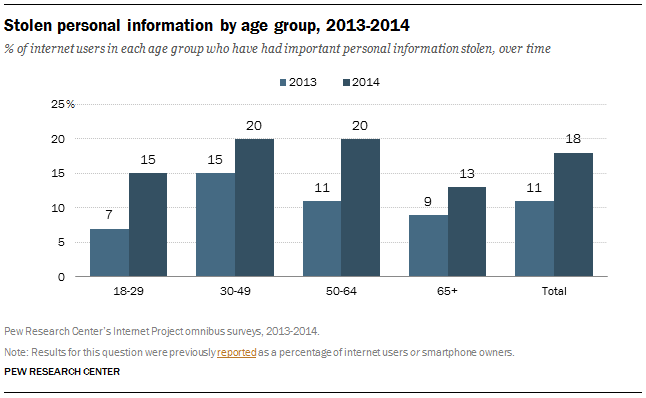
Achieving this goal would be a great advancement towards reducing cyber-attacks on business’ big data and cloud platforms. This would be transformative for industries that are usually hit by cyber-attacks. Increasing the confidentiality of big data would be the first step in carrying out this process. The confidentiality of big data would decrease the rate at which hackers get hold of people’s personal information. Also, it will create an awareness to people not to provide their personal information to unknown numbers or text messages. Protecting big data from unauthorized access by encrypting or putting more secured passwords on big data would prevent easy access by hackers. People should make their passwords more unique which would make it difficult to break. Furthermore, there should be proper firewalls built on industries’ network connections to detect IP address and network information of hosts or users connected to the network. This would help industries monitor and audit login of users. If such goals are implemented, industries can track new login or users to make sure it’s safe and would not affect the security of their big data. The integrity of the industries’ big data becomes secured and protected. These goals will take some months to develop, but the rewards from implementing the goals would be immense. Now, it is time to implement these strategies and prevent cyber-attacks on big data.

# Protecting Sensitive and Personal Information

Hackers usually attack several businesses due to businesses’ improper ways of protecting sensitive and personal information. See Appendix A for information on different industries affected by hackers’ data breaches. Sometimes customers also leave their personal information on fake websites and platforms. Hackers recover this information for cyber-attack purposes (4).

There are several vulnerabilities that hackers use to launch cyber attacks on businesses for their big data. First, hackers find it easy to break passwords that are not usually changed and are without multiple letters, numbers and symbols. Hackers can use different advanced technologies to break weak passwords to get hold of customer or business data(4). Hackers sometimes make unsolicited phone calls asking customers or businesses to provide personal information or re-submit login or password information. If hackers get hold of customer or business password information, they can launch cyber attacks on the business’s data especially via cloud platforms (1). Furthermore, hackers can access confidential data such as W-2s, social security and credit card numbers when they are sent by customers or businesses via email or phone numbers. See figure 1 for examples of stolen personal information of internet users. The lack of effective training for businesses and customers about preventing hackers and cyber criminals leads to more cyber-attacks (4). See Appendix B for data breaches over different years.

## Figure 1: Personal information stolen by hackers

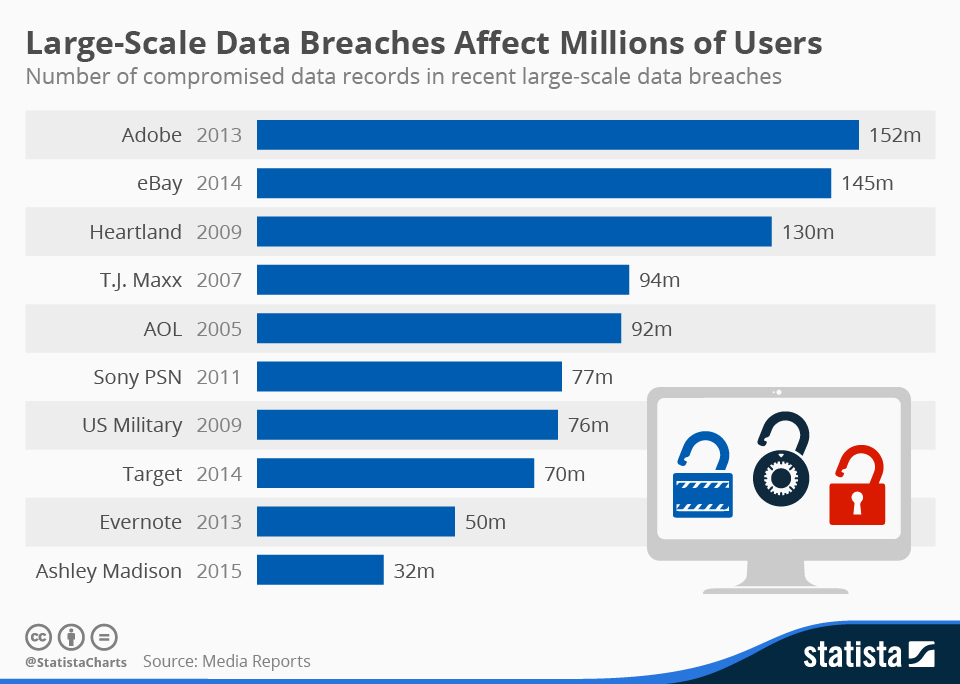


SOURCE: Pew Research Center. Pewresearch.org

# Lack of Big Skilled Data Security Professionals

Businesses need skilled professionals who can process and train other employees on data cyber-attacks and threats, and analyze large amounts of data. It is becoming difficult for businesses to find the right personnel who can ensure companies’ big data are safe (1). Over the years, hackers have exposed several vulnerabilities about the technologies and security tools used to process big data and prevent cyber-attacks. However, with the right skilled personnel and training, businesses would be able to take care of the vulnerabilities[[1]](#footnote-1) (4). Without data scientists[[2]](#footnote-2), data engineers[[3]](#footnote-3) and data security experts to design analytics applicable to big data with privacy requirements, hackers can have easy access to the data since there is no strong authentication models built by data engineers or scientists to protect big data (4). See figure 2 for large breaches on data sets at different companies. At these companies, the amount of breached data is shown in the graph.

## Figure 2: Large Sets of Data Processed by Data Engineers



Source: Statista Media Reports, https://www.statista.com/chart/2540/data-breaches/

# Solutions

Currently, the two best methods for protecting big data on cloud platforms from cyber attacks are increasing big data security and avoiding phishing attacks and emails.

# Increasing Big Data Security

Hackers target big data sets on cloud platforms because not only do they get more rewards, but they also penetrate different security layers that enable them access confidential company information (4). Companies have a lot at stake when hit by cyber-attacks. There are several ways that businesses can protect their big data on cloud platforms. First, businesses should collaborate with other industry peers to create industry standards, regulations, and best practices (4). This will help protect companies’ big data by ensuring that all businesses are obeying the security rules and regulations. Furthermore, companies should establish an attribute-based encryption to protect sensitive information. Companies should encrypt all their sensitive data. Hackers are not able to access encrypted data. Companies should securely encrypt passwords and implement security questions on all sensitive information to make it inaccessible to hackers (4). Companies should maintain and monitor audit logs across all their departments to check details of all individuals who login into the companies’ systems. This improves the security systems and ensures only authorized users log into their accounts (4).

# Benchmark: Capital One Data Breach

Capital One is one of the largest consumer banks in the U.S with over 50 thousand employees and approximately 28 billion US dollars in revenue in 2018 (5). It values the use of technology and is one of the earliest US banks to adopt cloud computing technologies. Capital One was one of the first banks to invest migrating their on-premises datacenters to a cloud computing environment. The data breach heavily impacted the migration (5).

In July 2019, Capital One disclosed an outside individual gained unauthorized access and obtained personal information of customers (5). Capital One disclosed that the personal information was customer’s data collected during credit card applications. The study proposed ways of improving Capital One’s big data security against data leak (5). There should have been an attribute-based encryption to block host access from the Internet Protocol Network and from malicious proxy server, alert successful access from malicious IP addresses, monitor and audit the use of administrative accounts and monitoring outbound traffic on the network (5). Capital One has used these different approaches to increase the security of their big data to prevent future cyber attacks on their big data (5).

# Avoiding Phishing Attacks and Emails

Phishing attack is a well-known type of cyber attack where scammers and hackers use email and text messages to trick people to give them their personal information or possibly install malware on the victim’s computer (6). These types of scams enable hackers and scammers to get access to the victim’s confidential information. Phishing attacks can come in several forms; they may look like an email from a known company with the company’s logo to make it look legitimate (6).

Phishing attacks can also come in a form of email asking users to click on a link to make payment and confirm personal information (6). Although phishing attacks may be difficult to detect, there are signs to detect an email or text message is a scam and should be avoided. Businesses should always check the “from” email address. This can help businesses detect if the email is coming from a legitimate source (6). Companies should look out for unsolicited emails with file attachments as such attachments when downloaded can infect the company’s big data with malware (6). Users should only download files from official websites. Companies’ workers should not trust any link that look suspicious, text messages with grammatical errors, and emails with general address such as “Dear recipient.”

# Benchmark: Protecting Your Organization from Cyber Attacks

In a study conducted by Gallagher, Cybersecurity in healthcare and senior living organizations, they illustrated the effects of cyber-attacks, phishing emails and ways of protecting organizations (2). The author of the case study, Jane Feagin, analyzed key points such as ransomware and how just clicking on a suspicious email attachment can open the company’s network for invasion. The author discussed how ransomware, a malicious software that encrypts victim’s data to make it inaccessible until an amount is paid, has become more common in the healthcare industry (2). The author analyzed that hacking accounts for over 45% of breach reports which impact companies with loss of millions of dollars (2).

Jane Feagin also studied avoided breaches. It is important to implement a cyber training program to educate workers on suspicious emails and phishing attacks (2). Workers should not use common passwords, never share passwords with anyone and never write password down to be saved at the workstation. This study pinpointed several ways to avoid phishing and malicious emails (2).

# Assessment

## Table 1

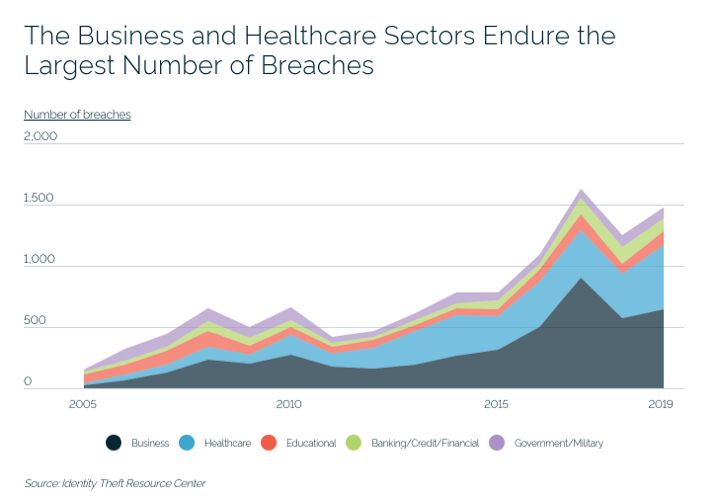
|  |  |  |
| --- | --- | --- |
|  | Increase Big Data Security | Avoid Phishing Attacks and Emails |
| Effective | Yes | Yes |
| Readily Available | Not always | Yes |
| Reduces Addition | Yes | Yes |

The two solutions from Table 1 have shown to be effective and have the potential to reduce cyber-attacks on big data. Unfortunately, not all the tools needed to increase big data security are readily available. Some of the security tools and practices are expensive to use and not all companies have the financial means to purchase such resource. This can change over time. If companies are given the needed training on the importance of big data security, they would invest good amount of money in purchasing security resources. Encrypting passwords and big data when stored has shown to be an effective way of increasing big data security which would reduce cyber-attacks on big data. Avoiding phishing emails has also shown to be an effective way of reducing cyber-attack on big data. Companies should train their employees on how to avoid phishing emails and stay on the lookout for potential phishing emails or text messages. These solutions reduce the addition or increase of cyber-attacks or malware on big data and should be seriously considered for big data’s security. Overall, these solutions show effective means of protecting big data’s security but will take months or years to fully implement into society or industries.

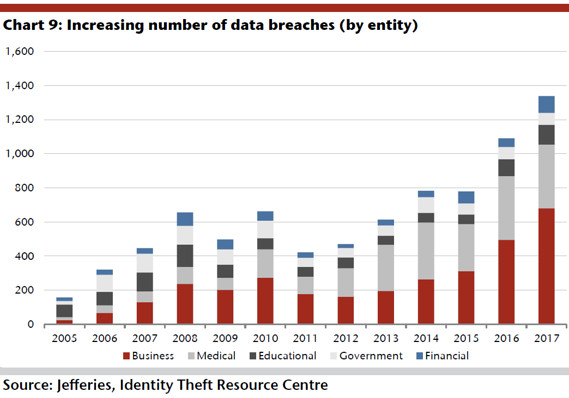
# Works Cited

1. Ardagna, Claudio A., et al. “Big Data Analytics-as-a-Service: Bridging the Gap between Security Experts and Data Scientists.” *Computers & Electrical Engineering*, Pergamon, 17 May 2021, <https://www.sciencedirect.com/science/article/pii/S0045790621002081>.
2. Feagin, Jane. “Protecting Your Organization from Cyber Attacks.” *Ajg.com*, https://www.ajg.com/us/news-and-insights/2021/sep/protecting-your-organization-from-cyber-attacks/.
3. Killion, Ben. “5 Cybersecurity Solutions for Financial Institutions.” *Aureon*, Aureon, 12 Aug. 2021, https://www.aureon.com/services/it-management/network/security/5-cybersecurity-solutions-to-benefit-your-bank/.
4. Moore, Michelle, et al. “Threat or Opportunity? Big Data and Cyber Security .” *University of San Diego*, 2 Dec. 2020, <https://onlinedegrees.sandiego.edu/threat-or-opportunity-big-data-and-cyber-security/>.
5. Neto, Nelson, et al. “A Case Study of the Capital One Data Breach.” *MIT MANAGEMENT SLOAN SCHOOL*, https://web.mit.edu/smadnick/www/wp/2020-07.pdf.
6. Payroll & HR, GTM. “Protecting Your Sensitive Data from Cyber Attacks.” *GTM Household*, 15 Dec. 2021, https://gtm.com/household/protecting-your-sensitive-data-from-cyber-attacks/.

# Appendix A: Business and Healthcare Breaches



# Appendix B: Data Breaches Over the Years



1. Flaws in the data’s security [↑](#footnote-ref-1)
2. Data Scientists interpret and extract meaning from data [↑](#footnote-ref-2)
3. Data engineers convert raw data into usable form [↑](#footnote-ref-3)