International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-9, Issue-2, April 2022
https://doi.org/10.55524/ijirem.2022.9.2.10
Article ID IJIRD-1169, Pages 78-83
www.ijirem.org

Google's Cybersecurity Framework

Ravindra Patel

Department of Computer Science, Campbellsville University, University Dr, Campbellsville, KY, USA 42718

Correspondence should be addressed to Ravindra Patel; ravipharmacy8@yahoo.com

ABSTRACT- Cybersecurity is a fundamental concept in modern-day organizations. Firms are constantly exploring security solutions to keep them secure from security compromises that bear a great potential of disrupting their daily operations. The cybersecurity landscape is highly diverse and incorporates numerous elements that firms can exploit to protect vital corporate systems, including networks and sensitive resources such as data. Google is highly conscious of cybersecurity and employs every measure to protect its vital IT resources and systems from security threats. Google's cybersecurity landscape is significantly mature and employs multiple plans that guarantee infrastructural security, data asset management, and effective access control. The firm's security policies greatly prioritize promoting employee security awareness as the firm understands that workers form a fundamental component of its entire cybersecurity plan. This paper explores Google's cybersecurity plan by focusing on cybersecurity security awareness programs, company information exposure on social networking sites, and the effects of not using encryption on network or Internet traffic. The paper will similarly recommend ways of minimizing information exposure while developing an understanding between password strengths and password managers in cybersecurity.

KEYWORDS- Google, Cybersecurity, Application, Network, Encryption, Software, Internet.

I. INTRODUCTION TO GOOGLE, AND ITS CYBERSECURITY INFRASTRUCTURE

A. Google Company Description

Larry Page and Sergey Brin founded Google Inc. in 1988. But later changed to Google LLC [8]. Google belongs to an industry that deals with various products and services, including the Internet, advertising, computer hardware, software, cloud computing, and Artificial Intelligence (AI). Google LLC, headquartered in California, U.S., is one of the prominent American multinational technology firms that focus on Internet-based products and services such as cloud computing, search engine, hardware, and software. The firm operates globally with approximately 140,000 employees and a revenue of nearly $190 billion [15]. Google's current parent company is Alphabet Inc. which helps Google organize its mission and meet its broader aspirations of making global information universally accessible and valuable.

B. Google's Cybersecurity Landscape

Google Inc. is one of the numerous firms in the world that are highly committed to cybersecurity. The firm's security strategy offers control to numerous data storage areas, data transfer, and access, making the primary touchpoints that hackers primarily target during attacks. The firm is guided by fundamental strategies that integrate multiple components, including data asset management, personnel security, disaster recovery, corporate security policies, business continuity, infrastructure security, and access control [5]. Google's security policy is clearly outlined in its Code of Conduct. It provides multiple security-based purviews spanning from general policies that target the workforce in their mission to comply with security standards to more specialized security policies that focus on the firm's internal systems that the firm's workforce is required to observe.

C. Google Security Policies

To ensure a successful cybersecurity plan, Google ensures that its security policies are regularly reviewed and updated. The primary reason for this undertaking is to ensure that the organization stays ahead of the arising potential threats and ensuring better compliance with IT security management within the firm [5]. Google also ensures that its employees undergo frequent security training on security matters such as safe use of the Internet, data labeling and handling of sensitive information and data, and safe remote working. Additional training is equally offered on security-related topics of concern, including critical fields of emerging technologies, secure utilization of mobile devices, and proper use of social innovations such as blogs and social networking sites.

D. Google's Information Security

Google has an around-the-clock Information Security Team that is well integrated into Google Software Engineering, comprising expert personnel in a wide range of information security management, including network security and application. This team is tasked with developing the firm's security review processes and constructing well-tailored security infrastructure for all its IT frameworks [5]. The team also documents and enforces the firm's security policies to ensure t firm is always informed of the latest security threats and developments. The firm's information security team conducts security designs, offers security plans for network frameworks, screens suspicious activities on the firm's networks, identifies and resolves information security compromises, and deliver workforce training on abiding with its security policies, particularly in fields of data security [5]. Other essential responsibilities of the information security team include running a vulnerability management program to identify network security concerns, involving external security professionals to perform regular security. Evaluations of the firm's IT infrastructure, and liaising with

software vendors to determine and resolve threats in third-party programs.

E. Google's Cybersecurity Plan

Google's cybersecurity plan forms a fundamental tool that helps the firm to protect its customers, workforce, and information. By underlining its cybersecurity setup's present and future environment, the plan delivers great clarity about Google's cybersecurity. It helps in ensuring the firm is always ready to resolve its cybersecurity issues. Google's cybersecurity plan is composed of the following vital components:

- Identification of critical assets and threats. Google has well identified the essential assets it needs protecting. The firm's threat and risk assessment and its progressive threat management process enable the firm to establish a safer cybersecurity environment [5]. Google's key assets include its network, cloud platforms, and data and are well covered in their cybersecurity plan.
- Prioritization of threats and assets. Google greatly prioritizes its asset and threats by employing the proper measures based on its IT context. The firm understands its security risks, explaining why the firm has effective countermeasures for every risk vulnerable to its systems and networks.
- Security goals. Google's IT security goals are highly achievable and realistic. The firm's policies and IT security approaches form its core cybersecurity plan since it outlines its activities on its cybersecurity journey. The isolation of activities and assigning them a specific period helps to identity the long and short-term goals that should be met based on their urgency.
- Documentation of cybersecurity policies. Cybersecurity marks one of the critical areas where it is vital to document policies and every step engaged during IT security. A cybersecurity plan offers a comprehensive toolkit that helps maintain cybersecurity best policies and related practices.
- Connecting security goals to organizational objectives. Google has a clear-cut business reason for every security goal that the firm has in place. In other words, the firm understands that every IT security tool employed should meet a specific goal towards the maintenance of a sound security environment. For example, Google's firewall is employed to facilitate easy access of the firm's employees to data while enabling them to undertake their work roles. The firm's cybersecurity plan has a significant impact on its products and services.
- Vulnerability testing. Conducting a vulnerability run is a sure way of identifying whether the cybersecurity plan is effective [16]. Google has mastered the vulnerability testing exercise where it regularly performs a vulnerability evaluation in its systems to minimize threat likelihood. The presence of Google vulnerability programs helps the firm to identify security threats in their systems and products, which helps towards vulnerability responses in the face of an attack.

After a given period, Google performs a cybersecurity assessment to ensure that its cybersecurity plan is relevant, updated, and effective. In this note, the firm often hires external experts to undertake regular security assessments, and at times penetration testing is performed to test the integrity of systems. Cyber threats are constantly evolving and adopting a reliable cybersecurity plan is essential to avert security vulnerabilities.

II. IMPLICATIONS FOR FAILURE TO USE ENCRYPTION ON NETWORK AND INTERNET TRAFFIC IN GOOGLE

Primarily, data transfers are conducted using either a private or a public network. Encryption on a network is essential because it permits data security so that no other party can access the data in a network [11]. Encryption on internet traffic facilitates secure communications by hiding what happens inside the organization's network [9]. When using traffic encryption, it becomes easier to avert viruses and malware. According to [1], related threat variants on the network, such as botnets, are mainly used to perpetrate Distributed Denial-of-Service (DDoS) attacks. At any given instance, encryption effectively prevents unauthorized users from eavesdropping on the firm's network traffic; regarding the network, encryption help in guaranteeing data security over an organization's shared communication network [10]. If no mechanisms are available to encrypt data and only HTTPS exists, such as in the case of Google, the data would be in readable format prior to being sent transmitted in the private network secured by a firewall. However, the data would not be secured and would most likely suffer from numerous security compromises.

In Google, security forms the top-most priority. The firm ensures that its services offer the most current HTTPS by default while ensuring its encryption activities are leveled on its products and services. HTTPS ensures that the content that the user views online is not eavesdropped on by unauthorized parties or altered by other individuals on the network [12]. According to [13], nearly 80 percent of Google Internet Traffic is encrypted. However, according to the firm, mobile devices, primarily older mobile devices that cannot support new standards and encryption protocols, are responsible for unencrypted end-user traffic [13]. Challenges in achieving full traffic encryption continue to lurk in other areas, especially those blocking HTTPS traffic. In other situations, insufficient technical resources in some organizations make it significantly challenging to implement Internet traffic encryption.

A. Cybersecurity Awareness Program

A cybersecurity awareness program is performed to educate the workforce on safeguarding their personal information and computer systems and protecting themselves from opportunistic cybercriminals searching the web for vulnerable users. Implementing a sound security awareness program will help the employees cultivate a security culture and minimize the chance of a security compromise. The security awareness program will incorporate multiple components to ensure that the awareness initiative succeeds and achieves the desired security objectives. The core components that the program will target include personnel roles, training selection, what to train, and ways to train.

B. Roles

When designing a security awareness program, it is crucial to highlight the critical roles to be managed in the program. In most cases, the rolls around the security awareness program will differ across organizations since the security objectives may appear different. Most of the efforts will be

centered on engaging with the workforce in communication and training. The manager and the Chief Information Security Officer (CISO) will be at the front line to facilitate the workforce's security awareness initiative. Preferably, a resource or department dedicated to researching, developing, and administering the roles and specifics of the program should carry forward the implementation of the security awareness program and its enhancement periodically. These personnel or the department also needs to hold a board-level managerial capacity or an equivalent responsibility within the IT field. The manager should dedicate their efforts to engaging the workforce in the relevant training to ensure they understand the basics of the IT infrastructure and other practical advanced security approaches critical in thwarting security compromises. CISO, on the other hand, is expected to offer adequate support towards the security awareness initiative. The security awareness manager should directly communicate with the organization's information security administrators, such as the CISO, to better coordinate the security awareness exercise. The CISO should be the most integral personnel in the program and be at the heart of the program's roles. The CISO has the capacity to offer guidance to the program and representing the program's objectives to the firm's top-most leadership. The advisory board should also be engaged during the awareness exercise. The Advisory board houses planning and steering committees who help establish the program goals for the success of the awareness program. The advisory board will assist the security awareness manager with crucial tasks such as planning, implementing, and managing an effective program.

C. Who to Train?

The primary goal of identifying the training group is to determine the type of training to be delivered, the mode of delivery, and the topics to be covered. Training will target the organization's workforce, who have limited awareness of the security landscape. During training, security policy, acceptable use policy, incident identification, reporting mechanism, and regulatory requirements such as HIPAA should be considered [6]. Different employee segments will be targeted, including full-time employees, privileged users, executives and their support staff, and temporary staff.

D. Full-time Employees

This group is required to complete compliance training specific to the policy requirements of the organization. The group should be trained to impart baseline behavioral expectations towards security for the organization's safety and as a compliance necessity.

The specific areas that need to be trained and focused on in this group include:

- Security Policy highlights
- Phishing training
- Acceptable use policy
- Regulatory requirements
- Ways to identify and report a security incidence.

These above training areas can also be applied and expanded to anyone working in any IT organization.

E. Privileged Users

These include users that possess privileged access to the organization's IT resources. Privileged users include system administrators, developers, network engineers, and database administrators. These personnel should receive technical training that aligns with their technical roles and incorporate the associated risk of their privileged access to IT resources. The group may be trained on password practices and management and software development life cycle.

F. Executives and Support Staff

The C-level executive roles and the roles occupied by the support staff are integral to the cybersecurity environment. These personnel factors as a significant risk directly affecting the firm owing to their daily work routine dealing with sensitive information. During training, the assistants should help train the executives since they offer vivid insights into the behaviors of the senior executive team.

G. Temporary Staff

Like other staff, the temporary staff is high-risk to the firm. In most cases, the temporary staff and contractors possess elevated network access but are usually not mandated by a similar training necessitates owing to legal, contractual restrictions. The temporary staff must be treated in a similar manner to other staff during training and should acquire proper training based on their access privileges and individual roles. The staff can be trained through the onboarding process and can be apprised on the password practices and management and security aspects that are industrially relevant.

H. What to Train?

Training should center on a small number of behaviors and areas of concern that present the most significant risk to the firm. The risks can be established by liaising with the Info senior leadership, reviewing past incidences that the workforce may have triggered, and analyzing industry reports. Besides, additional topics may be necessary for regulatory requirements. Essential cybersecurity awareness training should incorporate ransomware, phishing, reporting, social media privacy, policies, online security, passwords, and Wi-Fi security.

I.Approach to Training

Knowing how to conduct the training will help in the delivery of a sound security awareness program. A vital strategic component is reflecting on the organization's information security communication plan and identifying how the plan relates to other objectives of the organization. Engaging the target audience is the first step towards successful training [3]. Here, the audience should be divided into two levels, namely organizational and individual. From the organizational perspective, the security awareness plan should engage the senior

Management fully, and the communication should demonstrate adequate support of the program's goals. Liaising with the senior leadership will help establish the opportunities to reinforce security awareness and desirable security behaviors. For example, utilizing all-hands meetings may greatly help identify security gaps and determine the right approach to better security. Regarding individuals, it is crucial to driving the training programs towards procuring security behaviors alongside introducing resources to nurture better security practices in the work environment.

J. Security Awareness Training Program

Essentials When rolling out the security awareness training exercise, it is advisable to incorporate productive training

approaches such as engaging content such as infographics and videos, measuring results using quizzes, small clear modules, and utilizing phishing simulation capabilities. Delivering small-sized videos, little infographics, and interactive training customized for each user's likely risks will help launch a security awareness training program successfully. By enforcing the identified steps, the organization can begin its journey to raising cybersecurity awareness. By following the highlighted steps, the organization will be guaranteed to deliver the highest quality training for its workforce. The overarching goal of the security awareness program is to convert the employees into assets rather than security liabilities. In the end, the organization will save significant time, valuable resources, and chances of experiencing a cybersecurity attack.

III. COMPARISON BETWEEN PASSWORD STRENGTHS AND PASSWORD MANAGER DETAILS PROVIDED (TABLE 1)

- Password strengths and password manager provides a reliable way of implementing system security.
- A password manager can automatically create a strong password due to a random password generation mechanism.
- A password manager can be applied when deriving a password entropy. Entropy refers to the password strength measure in terms of characters used and the overall password length.

Table 1: The Contrast between Password Strengths and Password Manager

Password Strength	Password Manager
It is measured based on password effectiveness against actions such as password guessing and brute-force attacks.	It is a software developed to allow users to generate, manage, and store their passwords for ease of logging into their online activities.
Its effectiveness is significantly determined by character length used, password length itself, and the different characters utilized	The encryption capacities determine its effectiveness. End-to-end encryption warranties data protection when the data is at rest and when being conveyed.
It is determined by the ownership and knowledge and how these factors are designed and enforced.	Password managers are distinguished depending on their capacities to offer audit reports, ease sharing passwords safely, and the maximum number of passwords that each password manager can store on a single device.

IV. MINIMIZING COMPANY INFORMATION EXPOSURE ON SOCIAL NETWORKING SITES

Social media platforms are one of the fertile grounds that an organization can use o market themselves to the outside world. Due to the high number of potential customers in social media networks, modern firms exploit social media platforms to advance their marketing campaigns to attract more potential customers to their businesses [14]. However, despite social media platforms being significantly valuable for increasing market reach, fostering client relations, and developing company brands, firms are advised to be wary of rising social media security threats. Several mitigation measures can be employed to reduce company information exposure on social networking sites, such as:

- Developing a social networking site policy. Implementing robust privacy and security policies can prove instrumental in mitigating exposure of vital information to social media platforms.
- Restricting access to social networking platforms. This move aims to facilitate social media data security [7]. In modern firms, the workforce usually serves as the weakest security link and a significant data breach source. Ensuring social networking sites are restricted can prove to be the best approach to prevent company information from being exposed in social media forums. A firm may consider revoking its social networking accounts' access for individuals who cease to be workers of an organization. Revoking access to social networking accounts should similarly apply when an employee shifts their roles to eliminate chances of perpetrating a cybercrime.
- Avoid passwords reuse or changing passwords regularly can help mitigate corporate information exposure to social networking sites. Ensuring a unique password is used for every social networking account will help shrink attack windows and inadvertent information exposure to social sites [4]. Using unique passwords and changing them regularly will also ensure that even if one site is breached, it would be difficult to access other social sites linked to the organization's account. Exercising good.

Password hygiene will ensure that vital corporate information is inaccessible to authorized parties, minimizing the risk of exposing such information to social media platforms.

Policies offer excellent guidance to the workforce and cover the entire purview of protecting a firm when utilizing social media. An example is the use of access control policies to prevent an organization's social media accounts from being attacked and its sensitive information from leaking to social platforms. Besides, implementing additional policies targeting data compliance can help avert the likelihood of sensitive data leakage through social media forums.

Raising security awareness through training can significantly help minimize sensitive company information exposure in social media forums. Security awareness will help instill a sense of responsibility among the users by sensitizing them on the do's and don'ts when interacting with social media platforms and sensitive corporate information [2]. Increasing security awareness will also help ensure that users are not lured by malicious personnel to give out vital company information or expose sensitive information over the network.

K. Google's security for US government

Black, White, or other community people will benefit from having a trustworthy company as their digital identity security increases. It is easy for the government to decide on a person applying for a passport or driving an armored car license plate. This initiative would enable the community to gain the most value from having the best available cybersecurity technology at their fingertips. The internet

grows and changes, and there will continue to be demand for IT security as new technologies and services emerge that may not be available to the public. Google's efforts will benefit the American community and the American public. Google has been at the forefront of developing new security software, making the American public a lot safer. Google's Cybersecurity will help to protect the American public from computer viruses and other dangerous online activity. One of the ways Google helps keep the American public safe is by teaching the American public about online safety. Google teaches Americans about ways to avoid cybercrime and keep their information safe. Black businesses are less likely to have a security program in place. Black businesses are less likely to have an on-site security force to respond to any emergency [7].

Black citizens are less likely to access public facilities. Some black and white groups in the USA are worried that they might lose control if a social security number or other personal information was lost or compromised. Black members seek information on cyber security, including their responsibilities, threats, and opportunities. The Cybercrime Threat In general, Black people have been victimized by cybercrime for centuries. Cybercrime affects Black people in every part of the world. It is essential that acknowledge that it is a global issue. It is a global problem where everyone is affected [7].

The US is the country that is known for its most advanced and complex computer systems. A single data center can be one of the most powerful, not to mention the Pentagon uses a sophisticated military computer system. Google is taking things a step further than usual by integrating them into a unified computing system, and it is like a national digital security network. Google Sandbox is used in security. Security measures for the sandbox: Sandbox is designed to secure data and prevent malicious actions. Sandbox is not accessible to the public. Sandbox users do not need to install a program. The developer or administrator controls the sandbox to prevent a security threat. Sandbox is designed to help researchers and security companies find new ways to resolve security vulnerabilities. Google is helping the US government to improve national security in many ways. They are creating the best security tools which can protect the entire infrastructure of the government. They even made the internet a very secure place. The government uses its services and applications through secure connections. The best part of their services is that their security protocols are very efficient [4].

V. CONCLUSION

Firms are presently finding themselves being highly pressurized to respond promptly to the highly rising cybersecurity threats. Modern attackers are constantly developing newer ways of compromising corporate systems, forcing organizations to devise stronger measures to mitigate these attacks. The cybersecurity plan marks one of the most resourceful strategies to countering attackers' efforts of lodging security attacks on vital organizational resources. Google has been at the forefront of implementing informed cybersecurity measures such as encrypting its network traffic and developing a cybersecurity awareness program. All these efforts are geared towards maintaining a secure environment free of security compromises. The enhancement to the cybersecurity posture of organizations and individuals bears tremendous importance towards minimizing the damage that comes with cybersecurity breaches.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my professor as well as our principal who gave me the golden opportunity to do this wonderful project on the topic Google's Cybersecurity framework which also helped me in doing a lot of Research and I came to know about so many new things. I am thankful to them.

REFERENCES

[1] Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet based distributed denial of service (DDoS) attacks on web servers: Classification and art. ArXiv Preprint ArXiv:1208.0403, 49(7).

[2] Aloul, F. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, 3(3), 176–183. https://doi.org/10.4304/jait.3.3.176-183

[3] Caldwell, T. (2016). Making security awareness training work. Computer Fraud & Security, 2016, 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

[4] Franchi, E., Poggi, A., & Tomaiuolo, M. (2017). Information and Password Attacks on Social Networks: An Argument for Cryptography. Journal of Information Technology Research, 8(1), 25–42. https://doi.org/10.4018/JITR.2015010103

[5] Google Inc. (2011). Security Whitepaper: Google Apps Messaging and Collaboration Products. http://webcache.googleusercontent.com/search?q=cache:BYArJhqP0wYJ:www.google.c om/a/help/intl/en-GB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf+&cd=1&hl=sw&ct=clnk&gl=ke

[6] Habitu8. (n.d.). Security Awareness Program Plan & Strategy Guide. Retrieved May 22, 2021, from https://info.habitu8.io/security-awareness-program-plan-and-strategy-guide

[7] Hiatt, D., & B., Y. (2016). Role of Security in Social Networking. International Journal of Advanced Computer Science and Applications, 7(2). https://doi.org/10.14569/IJACSA.2016.070202

[8] Hosch, W. L. (n.d.). Google | History & Facts. Encyclopedia Britannica. Retrieved May 22, 2021, from https://www.britannica.com/topic/Google-Inc

[9] Kumar, M., & Kishor, A. (2019). Network Traffic Encryption by IPSec. International Journal of Computer Sciences and Engineering, 7(5), 912–915. https://doi.org/10.26438/ijcse/v7i5.912915

[10] Lakhtaria, K. (2011). (PDF) Protecting Computer Network with Encryption Technique: A Study.

[11] International Journal of U- and e- Service, Science and Technology, 4(2). https://www.researchgate.net/publication/226217163_Protecting_Computer_Network_with_Encryption_Technique_A_Study

[12] Lopatto, E. (2014). What is HTTPS and why does Google like it so much? —Quartz. https://qz.com/246441/what-is-https-and-why-does-google-like-it-so-much/

[13] Moscaritolo, A. (2016). 77 Percent of Google Internet Traffic Now Encrypted. PCMAG. https://www.pcmag.com/news/77-percent-of-google-internet-traffic-now-encrypted

[14] Ohajionu, U. C., & Mathews, S. (2015). (PDF) ADVERTISING ON SOCIALMEDIA AND BENEFITS TO BRANDS. Journal of Social Sciences and Humanities, 10(2). https://www.researchgate.net/publication/299561852_ADVERTISING_ON_SOCIAL_MEDIA_AND_BENEFITS_TO_BRANDS

[15] Statista. (n.d.-a). Google: Annual revenue. Statista. Retrieved May 22, 2021, from

https://www.statista.com/statistics/266206/googles-annual-global-revenue/ Statista. (n.d.-b). Number of Google employees 2018. Statista. Retrieved May 22, 2021, from https://www.statista.com/statistics/273744/number-of-full-time-google-employees/

[16] Yaqoob, I., Hussain, S., Mamoon, S., Naseer, N., & Akram, J. (2017). Penetration Testing and Vulnerability Assessment. Journal of Network Communications and Emerging Technologies (JNCET), 7(8).

ABOUT THE AUTHOR

Ravindra Patel was born in Karjan town, Vadodara city, Gujarat, India in 1985. He received the B.S. in Pharmacy and M.S. degrees in Technology Management, Professional MBA, and Computer Science from the Campbellsville University, KY, USA in 2022. Since last 4 years he has been working as data analyst and I am passionate about data.