

ASSIGNMENT COVER LETTER

For use with online submission of assignments

Unit Name: Advanced Cybersecurity

Unit Code: ISYS6002

Assignment No: 1

Assignment Tittle: Critical Review

Student name: Kashaboina Tharun Kumar

Student ID: 24137157

**Table of Contents**

[Introduction 1](#_Toc135397514)

[Outline 1](#_Toc135397515)

[Personal Identifiable Information (PII) 1](#_Toc135397516)

[CIA 2](#_Toc135397517)

[Threats and Vulnerabilities 3](#_Toc135397518)

[Protections 3](#_Toc135397519)

[Lessons Learnt from the Breach 4](#_Toc135397520)

[Organization’s Action after the Breach 5](#_Toc135397521)

[Importance of the Breach 5](#_Toc135397522)

[Conclusion 6](#_Toc135397523)

[References 7](#_Toc135397524)

# Introduction

This assignment is about conducting an in-detailed discussion in cybersecurity incident case study of Ring Home security camera breach. This paper has identified the Personal Identifiable Information or PII, which is held, collected and used by the organization. Moreover, CIA triad has been discussed and how these principles relate to the selected security breach have also been portrayed. This assignment has also identified vulnerabilities and threats explored in the case study. Furthermore, important protections that are applicable to resolve the cybersecurity issues associated with the smart security camera.

# Outline

Ring home is an Amazon owned organization, which manufactures and sells cost-effective and motion activated security cameras for maintenance and easy installation. This camera accidentally revealed user data to both Google and Facebook through third party trackers embedded into their android application (The Guardian, 2023). In another incident, same was happened as a result of an IoT breach whereby cybercriminals successfully hacked into home monitoring systems and connected doorbell of several families (The Guardian, 2023). This particular case study has been chosen because it would develop a clear idea about cybersecurity risks associated IoT systems.

# Personal Identifiable Information (PII)

PII or Personal Identifiable Information is referred to the representation of any information, which allows an individual’s identity to whom the information applies to be inferred reasonably by either indirect or direct means (Lee, 2020). Ring and its parent company, Amazon held, collect and use the name of the user, his or her email, phone number and postal address as PII. In addition, this organization also knows the geolocation of the phone connected with the camera, signal strength, information regarding Wi-Fi network, model of the camera, serial number and so on (Dhirani, Armstrong & Newe, 2021). Therefore, Ring camera retrieve information regarding the carrier and device along with the unique identifiers, which permit to track the users through real-time transaction data with the app and information regarding the home network (Lee, 2021).

# CIA

CIA triad is the abbreviation of Confidentiality, Integrity and Availability. It is considered to be a common model, which forms the basis for the security system development (Datta Burton et al., 2022). It is mainly utilized in order to explore the methods and vulnerabilities in order to create solutions. Cybersecurity risks majorly enter through the internet network. Inbound traffic can be riddled with social engineering schemes and potential malware (Medoh & Telukdarie, 2022). Without any control, outbound traffic can result in the users to access the insecure websites and expose a company to the security attacks. The IoT devices allow physical things or objects to exchange and collect information and such devices always risk prone (Lee, 2020). Ring home camera is also an IoT system. It creates significant scope for entrance for these hackers for getting enough information and performing their exploits. Ring camera can be given a unique identifier and it has the capability of autonomously communicating over the local network or internet. Therefore, such smart camera is prone to attacks, which can expose potentially private information. Furthermore, the ring home camera is embedded with low memory processors, which set a limit on the capability of processing information at high speeds that hinders the effort for maintaining integrity and confidentiality of this device. The IoT security breach associated with Ring home camera is always considered to be the reminder to the users to remember to change the credentials of admin while receiving the new smart hardware and adhering the fundamental rules of cybersecurity following CIA Triads like creating unique login details (Dhirani, Armstrong & Newe, 2021).

# Threats and Vulnerabilities

The threats and vulnerabilities associated with the Ring home cameras are as follows:

1. Use of Outdated or Insecure Components: This threat associated with the Ring home camera includes the use of third-party hardware components from a compromised supply chain (Lee, 2021).
2. Insufficient Protection of Privacy: The personal information of the users of Ring home camera are stored on the device, which is utilized improperly, insecurely or without permission.
3. Insecure Storage and Data Transfer: Lack of access control and encryption of sensitive data including in transit, at rest or during processing anywhere in the device is a huge threat (Datta Burton et al., 2022).
4. Lack of Device Management: Lack of security support is a huge concern for smart cameras. This issue is deployed in secure decommissioning, response capabilities and systems monitoring (Medoh & Telukdarie, 2022).

# Protections

Ring home camera has expended its end-to-end encryption for protecting its users. Ring Protection Plan has been taken into consideration to mitigate the cybersecurity concerns. It is an optional subscription, which provides the users with the access to paid features for Ring devices like alarms, cameras and video doorbells (Lee, 2020). With this plan, users can review, save and share videos from the Ring cameras to their Ring accounts.

Ring has used high-powered processors to mitigate the scopes of attacks (Mashable, 2023). However, this protection technique has come up with a loophole. The attackers always seek to utilize the power of the processors within the cameras as a tool. It is not a direct attack and the individual or organization using such cameras may not experience a data breach (Dhirani, Armstrong & Newe (2021). Nevertheless, their resources can be utilized by the outside sources and such action can be tracked back to the processor of their devices. Therefore, it is still not very ideal for the Ring home cameras.

# Lessons Learnt from the Breach

The security breaches associated with the Ring home camera has developed a consciousness about the legal and financial aspects and risks associated with the smart cameras (Datta Burton et al., 2022). The critical legal issue associated with Ring home camera is that recording usually needs the consensus of all the parties to be recorded and monitored. It implies that everyone has the right to enjoy a reasonable privacy expectation. It has several repercussions to use smart cameras. The Electronic Communication Privacy Act of 1986 prohibits audio communications’ interceptions without consent, but it does not address the video recordings (Digital Trends, 2023).

The rapid occurrence of security attacks creates a reliability issue among the customers. The similar incident has been taken place against Ring after the two cybersecurity breaches (Medoh & Telukdarie, 2022). Ring had to face a great financial loss because the sales volume was decreased after the consecutive two security breach incidents. Amazon and Ring, both had lost their potential customers. Therefore, Amazon faced a great decline on the graph of profitability and revenue generation from the sale of the smart cameras.

# Organization’s Action after the Breach

After the breaches, Ring has created law enforcement partnerships that have allowed users for sending photos and footage to the polices in more than 1300 cities (Digital Trends, 2023). Moreover, Ring has come up with a protection plan to deal with malicious attacks and vulnerabilities. This plan is nothing but an optional subscription, which would give an access to the paid features for all the devices manufactured and sold by Ring including alarms, cameras, doorbells and video. In addition, Ring has fixed sneakily fixed the security vulnerabilities in its Android application, which could have exposed the recordings of the camera of users including phone number, email, full name, camera recordings, address and geolocation (Mashable, 2023). With the help of this app, the footage of the device is stored in the cloud or in an infamously easy-to-hack space that can be accessed by Amazon employees (Mashable, 2023).

# Importance of the Breach

The security breaches encountered with the Ring home security cameras have shown the importance of privacy protections (Datta Burton et al., 2022). These incidents have opened up the eyes of the manufacturer and seller. Amazon and Ring collaboratively have compelled to strengthen the privacy of these cameras. In this regard, Ring has developed Ring Protect Plan which creates a huge scope for the users to share, review and save video recordings from the Ring devices to their Ring account. These incidents have made a strong realization for Ring to utilize high powered processors in Ring home cameras to strengthen its privacy and integrity (Dhirani, Armstrong & Newe, 2021).

# Conclusion

The entire study has enlightened the severity of cybersecurity vulnerabilities that can hamper the privacy, confidentiality and integrity of smart devices. Therefore, this paper has successfully depicted the PII along with discussing CIA triad and the relation between the CIA triad with the security breaches encountered against Ring security camera. Moreover, this paper has successfully portrayed important protections that would secure the privacy aspects of these smart cameras. Furthermore, this paper has successfully enlightened the lessons learnt from the security breaches.

# References

Datta Burton, S., Tanczer, L. M., Vasudevan, S., Hailes, S., & Carr, M. (2022). The UK Code of Practice for Consumer IoT Cybersecurity: where we are and what next. <https://gala.gre.ac.uk/id/eprint/38567/1/38567_VASUDEVAN_The_UK_code_of_practice_for_consumer_IoT_Security.pdf>

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), 3901. <https://www.mdpi.com/1424-8220/21/11/3901/pdf>

Digital Trends. (2023). *What You Need to Know about Smart Camera Privacy,* Retrieved from: <https://www.digitaltrends.com/home/what-you-should-know-about-smart-camera-privacy/>

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157. <https://www.mdpi.com/1999-5903/12/9/157/pdf>

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. <https://e-tarjome.com/storage/btn_uploaded/2021-06-15/1623738581_11813-etarjome%20English.pdf>

Mashable (2023). *Amazon Sneakily Fixed a Vulnerability In The Ring Camera*. Retrieved from: <https://in.mashable.com/apps-and-software/37018/amazon-sneakily-fixed-a-vulnerability-in-the-ring-camera>

Medoh, C., & Telukdarie, A. (2022). The future of cybersecurity: a system dynamics approach. *Procedia Computer Science*, *200*, 318-326. <https://www.sciencedirect.com/science/article/pii/S1877050922002393/pdf?md5=adf72cea6baf2f5fc5a98cddf3bfd5d0&pid=1-s2.0-S1877050922002393-main.pdf>

The Guardian (2023). *Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs.* Retrieved from: <https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats>