

A Security Approach: Principles and Practices of the Data Security, Governance and Compliance

1st Given Edward Patch

Software Engineering and Artificial Intelligence (of MSc Year 4)

Data Security, Governance and Compliance

University of Wales Trinity St. Davids (of Dr. Carlene Campbell)

Swansea, Wales

Student ID: 1801492

Abstract—Scenario Provided: CoffeeBlend provides Jamaican coffee services to a local and global market, including a high online and social media presence. CoffeeBlend uses Cloud Services to deliver services to the company's staff and clients. CoffeeBlend's network is ninety-five per cent wireless based, with a large amount of traffic receiving and transmitting data whether the data is client, staff or other forms of Intellectual Property. As the company lacks a Security Policy, it is vital to guarantee that CoffeeBlend's Security Policy stands in place to ensure the data of CoffeeBlend remains intact and gives the company's consumers and staff security. The research paper focuses on the current infrastructure of CoffeeBlend by conducting tests to find any potential data leaks and forming a Security Policy to protect the client's and staff's devices and data from any form of access.

Index Terms—Security, Framework, Infrastructure.

I. INTRODUCTION

This research paper covers the necessary details to understand the current infrastructure's security flaws and establish a Security and Bring Your Own Device (BYOD) Policy to protect the Intellectual Property from access outside and inside the system. With CoffeeBlend rapidly growing online and using Cloud Systems, the business will most likely suffer from incorrect security group configuration, data breaches, unauthorised access and insecure APIs.

Furthermore, a necessity for a Security Policy revision is in position as the policy is unavailable. The revision plan includes CoffeeBlend's compliance, risk management and Service Level Agreement (SLA); the laws and ethics; current and future risks assessment; the requirements to keep the Security Policy up-to-date and under any mentioned laws.

Researching the mentioned security models and any additional ones would benefit the Security Policy creation. In addition, using security models similar to the International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) [1], Security Technical Implementation Guides (STIGs) [2], and National Institute of Standards and Technology (NIST) 800-61 [3] would help speculate and formulate a network Security Policy and topology plan. Including the governance and compliance of the Security Policy and current network procedures to futureproof CoffeeBlend's Intellectual Property, including consumers and employees.

II. RESEARCH BACKGROUND

A. Cloud Security

Many organisations trust Cloud usage, believing that the Cloud Company ensures the data is stored, accessed and processed on the cloud system. However, this statement is not valid. Cloud Computing Companies, for example, Amazon Web Services (AWS), provide many different Cloud Services and Building Tools that offer the customisation of varying Security Policies and Access Methods, giving control to the consumer. The available flexibility of the Cloud Services moves the liability away from the Cloud Computing Service provider as the user should set the Cloud Service correctly, conditioned to the Use Case.

Amit Hendre and Karuna Pande Joshi [4] research some of the few key risks and with suggestions of security models, including data breaches, data loss, account or service traffic hijacking, insecure interfaces and Access Point Interfaces (API) and Denial of Services (DoS) shared technology vulnerabilities as a possible risk of Intellectual Property. The table found within the Journal Article [4] recommends different Security Models for the mentioned cloud vulnerabilities. Table I lists three of the recommendation's for the listed cloud vulnerabilities from the 'A Semantic Approach to Cloud Security and Compliance' - Amit Hendre and Karuna Pande Joshi [4].

TABLE I
RECOMMENDATION OF SECURITY COMPLIANCE MODEL-BASED ON
SECURITY THREAT - AMIT HENDRE [4]

Type of Threat	Recommended Security Compliance Model
Data breaches	STIG [2], ISO-27001 [1], ISO-27002 [5]
Data loss	STIG [2], NIST 800-61 [3], ISO-27002 [5]
Account or Service Hijacking	STIG [2], ISO-27002 [5], NIST 800-61 [3]
Insecure Interfaces/API	OASIS and OVF [6], FIPS 140-2 [7], ISO-27002 [5]
DoS	PCI DSS [8], ISO-27001 [1], NIST 800-61 [3]

B. BYOD Security

As cliental and employees can both bring their devices to CoffeeBlend's business, it is important to conduct an risk assessment. This risk analysis prevents any potential security flaws within the system protecting both cliental and

Intellectual Property. A series of questions are evaluated within the 'Risk Assessment of BYOD: Bring Your Own Device' authored by Shigeaki Tanimoto, Susumu Yamada, Motoi Iwashita and Toru Kobayashi [9], some of the picked evaluations are shown below, which will help assess the current security infrastructure.

“(Enterprise Side - System) - Unauthorised access via BYOD - Risk Mitigation.

(Enterprise Side - System) - An employee's private data mixture in a BYOD terminal - Risk Acceptance.

(Enterprise Side - System) - The leak-of-information issue of the in-company data of confidential information - Risk Transference.

(Enterprise Side - System) - Computer virus infection by unsuitable software etc. - Risk Transference.

(Enterprise Side - System) - Decision and education of the Security Policy of BYOD introduction - Risk Mitigation.

(Enterprise Side - System) - URL connection destination restrictions of BYOD - Risk Mitigation.

(Employee Side - System) - Data leakage risk from BYOD during Cloud use - Risk Transference.

(Employee Side - System) - Shoulder hacking of BYOD by others - Risk Acceptance.

(Employee Side - System) - Leak of information during connection to public Wi-Fi environment etc. - Risk Transference.

(Employee Side - System) - The pass code of BYOD is not set up - Risk Acceptance.

(Employee Side - System) - Use of BYOD by family etc. - Risk Acceptance.” - Shigeaki Tanimoto [9]

Risk Avoidance indicates that there is a way of avoiding the risk. **Risk Mitigation** means that it is essential to reduce the risk. **Risk Transference** moves the responsibility to a third party. **Risk Acceptance** suggests accepting the risk unconditionally.

C. Compliance

Without a Security Policy and a global market, mistakes are only a matter of time. With different regional laws protecting the consumer put CoffeeBlend into a legal situation. The two focused on EU and UK legalisations.

CoffeeBlend's digital data, including Intellectual Property, is currently volatile due to the data stored and processed on Cloud Services with little-to-no security. If a UK consumer's data leaks, it impacts the Data Protection Act 2018 [10]. However, if the consumer is under the EU legalisation, it can infringe the General Data Protection Regulation (GDPR) [11].

The Data Protection Act 2018 [10], formerly versioned as The Data Protection Act 1998, is now revisioned to accept the GDPR laws allowing businesses to follow the EU guidelines easier without having to conduct additional research, burning time and resources.

The laws of The Data Protection Act [10] that any use of any data from a consumer should stand: fairly, lawfully and transparently, specified and explicit purposes, adequate,

relevant and limited to what is necessary; kept up-to-date, kept for a short time frame, handled with the appropriate security with the upmost protection to protect against unauthorised data breaches; involving access, data loss, destruction or damage. The act mentions that handling sensitive information, including race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health and sex life or orientation has separate safeguards relating to criminal convictions and offences. CoffeeBlend should always inform the UK-based consumer of:-

- information about the way their data is processed.
- control to their data (updating incorrect data, erasing data, stopping or restricting the processing of their data).
- data portability from CoffeeBlend's organisation to another in a safe manner.
- cancellation of any process in that they feel their data is compromised.

Even though UK's Data Protection Act 2018 [10] implements the EU's GDPR [11] laws, it still lacks to acknowledge other crucial points found within the GDPR [11] law. Similarly to The Data Protection Act 2018 [10] it is vital to inform citizens and customers of any activity involving their data. The Policy Privacy should include this information in the most transparently available. Assignment of a Data Protection Officer (DPO) that reports and takes responsibility for the Data Protection Authority in the country that the organisation situates. To refer to the DPO-related rules, check Article 37-39 GDPR [11]. A requirement for a Data Processing Agreement (DPA) should initiate with any Third-Party data handlers to keep a backlog of where the data went and why it went to the destination for consumer safety.

III. SECURITY FRAMEWORK

There are many security guidelines with different and similar security approaches. Thus, it is imperative not to clash with security framework models. CoffeeBlend's Security Policy should adopt at least a few recommended security models to protect the network from covering itself legally and ethically.

STIGs [2], NIST 800-61 [3], and ISO-27002 [5] are the common standards to cover the type of threats found within Table I, including data breaches, data loss, account and service hijacking, insecure interfaces/API and DoS.

STIGs [2] helps add to the security of data breaches, data loss and account or security hijacking.

ISO-27002 [5] focuses on the threats of data breaches, data loss, account or service hijacking, insecure interfaces/API providing a wider area than STIGs [2].

NIST 800-61 [3] provides coverage for data loss, account and service hijacking and DoS.

Recommendation of ISO-27002 [5] and NIST 800-61 [3] to create the security framework as the ISO-27002 pushes security for the five selected threats that CoffeeBlend will suffer the most. NIST 800-61 [3] delivers security for the DoS threats. The security framework is as when CoffeeBlend expands, and the company will most receive threats from these

selected categories. The narrowed-down selection of ISO-27002 [5] and NIST 800-61 [3] is a maintainable framework.

IV. SECURITY INFRASTRUCTURE

Figure 1 contains the current network infrastructure of CoffeeBlend. The diagram helps highlight potential security issues with the network infrastructure, including the Local Area Network (LAN) and Cloud Services. Focusing on the LAN network, the infrastructure found in CoffeeBlend's business uses a router providing internet access, a switch allowing connectivity to four employee computers and a Home Router. The Home Router delivers wireless access to employee and consumer devices.

Another note to make, the Home Router has a password, 'ABCDEFGH', for the employees and a Guest WiFi channel with no security in place. On top of this, figure 2 shows that the Guest WiFi allows access to other devices within the network. This issue will enable hackers to connect to not only other consumer devices but also to employee BYOD devices and intellectual employee computers within the network. These cases are considered **Risk Mitigation** [4] falling under the 'Unauthorised access via BYOD' category and **Risk Acceptance** [4] falling under the 'An employee's private data mixture in a BYOD terminal' category. A way of solving this issue is to use WPA2-Enterprise login for employees and a separate network for the Guest network with no requirements for the authentication policy.

The current scenario shows three consumers connected to the LAN network; two smartphones named 'Hack4Fun-PH' and 'DavidPrice-SP' and a laptop named 'Kali-Laptop'. These names display the situation and likely would not be the case outside this portrait. The 'Hack4Fun-PH' would have access to 'DavidPrice-SP', and with more additional knowledge, they can connect to 'Emily-Phone', 'Thomas-LPC' and 'Thomas-TPC' devices. The user may struggle to communicate with the employee PCs. However, depending on the PC firewall setup and Smartphone software, it is still very much possible. The 'Kali Laptop' suggests that the consumer's laptop contains software that exploits the system's security. An operating system like the Linux Distribution, 'Kali' for example, has packages installed that would sniff any system deficiencies, telling the user of the Security Policy in position and even acquiring access to the entire infrastructure of the network.

A crucial problem with the infrastructure is outside of the network. Assuming that 'CloudExploiter-PC' is hacking CoffeeBlend's Cloud Services and 'DeviceHacker-PC' is hacking CoffeeBlend's LAN. The 'DeviceHacker-PC' can get into the network as no firewalls protect any devices registered onto CoffeeBlend's network. Under similar circumstances of the 'Unauthorised access via BYOD' (**Risk Mitigation**) [4], 'Shoulder hacking of BYOD by others' (**Risk Acceptance**) [4], and 'The leak-of-information issue of the in-company data of confidential information' (**Risk Transference**) [4] categories. The addition of Firewalls within the network reduces the chance of each risk occurring. Whether or not the attacks are outside or inside the network.

The 'CloudExploiter-PC' can penetrate the Cloud Services by finding improper configurations or disrupting the network by DoS, causing CoffeeBlend to suffer financially. One thing to mention is that if 'CloudExploiter-PC' gains access to the Cloud Services, the user may gain knowledge of consumer data and IP addresses to connect to the central infrastructure.

The firewalls in front of the two devices within the diagram suggest good security from the hacker's point of view to make tracing back hard. The network the exploiter devices are on would primarily be using a Virtual Private Network (VPN) to disguise the identity and IP address.

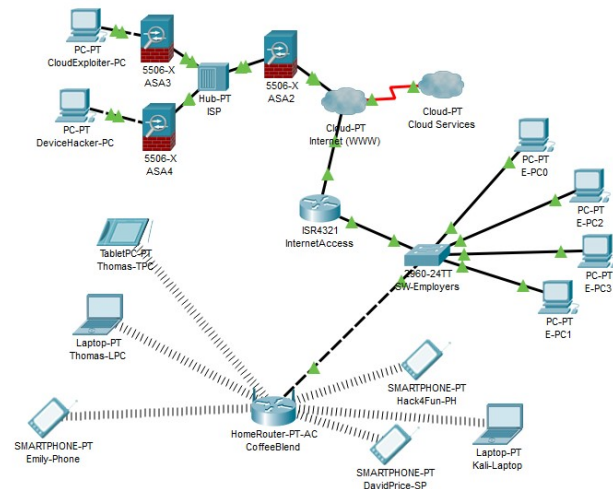


Fig. 1. CoffeeBlend's Network Infrastructure

V. CONCLUSION

The Security Policy includes ISO-27002 and NIST 800-61 to protect CoffeeBlend's networks from data breaches to DoS and security infrastructure recommendations keeping close to compliance and governance. It is vital to have a Security Policy in position early on, even with a minimal network, as any attacks on the network move all blame to the company.

CoffeeBlend must ensure they meet the security framework, infrastructure and legal requirements. A significant security issue lies in the internal network with zero consideration of BYOD and external security.

VI. TERMINOLOGY

List of terminologies used in this document:-

- BYOD - Bring Your Own Device.
- SLA - Service Level Agreement.
- ISO - International Organisation for Standardisation.
- IEC - International Electrotechnical Commission.
- STIGs - Security Technical Implementation Guides.
- NIST - National Institute of Standards and Technology.
- AWS - Amazon Web Services.
- GDPR - General Data Protection Regulation.

☒ Allow guests to see each other and access the local network

2.4 GHz

☒ Enable Guest Profile

Network Name (SSID):

☒ Broadcast SSID

Security Mode: Disabled

5 GHz - 1

☒ Enable Guest Profile

Network Name (SSID):

☒ Broadcast SSID

Security Mode: Disabled

5 GHz - 2

☒ Enable Guest Profile

Network Name (SSID):

☒ Broadcast SSID

Security Mode: Disabled

Fig. 2. CoffeeBlend's Network Infrastructure

- DPO - Data Protection Officer.
- API - Access Point Interface.
- DoS - Denial of Service.
- LAN - Local Area Network.

VII. REFERENCE LIST

- [1] ISO27001, "ISO/IEC 27001:2022." [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/28/82875.html>
- [2] "Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange." [Online]. Available: <https://public.cyber.mil/stigs/>
- [3] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP) 800-61 Rev. 2, Aug. 2012. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- [4] A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," in *2015 IEEE 8th International Conference on Cloud Computing*, Jun. 2015, pp. 1081–1084, iSSN: 2159-6190.
- [5] ISO27002, "ISO/IEC 27002:2022." [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/56/75652.html>
- [6] "Compliance | Information Management Services." [Online]. Available: <https://www.oasisgroup.com/compliance/>
- [7] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, Feb. 2020, pp. 1–3.
- [8] "PCI DSS Compliance Solutions & Services | AT&T Cybersecurity." [Online]. Available: <https://cybersecurity.att.com/solutions/pci-dss-compliance>
- [9] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato, and A. Kanai, "Risk assessment of BYOD: Bring your own device," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Oct. 2016, pp. 1–4.
- [10] "Data Protection Act 2018," publisher: Queen's Printer of Acts of Parliament. [Online]. Available: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
- [11] "GDPR Archives." [Online]. Available: <https://gdpr.eu/tag/gdpr/>
- [12] "Assessment of Information Security in Integrated Systems | IEEE Conference Publication | IEEE Xplore." [Online]. Available: <https://ieeexplore-ieee-org.ezproxy.uwtsd.ac.uk/document/9642824>
- [13] W. Najib, S. Sumaryono, L. E. Nugroho, and G. D. Putra, "Development of Enterprise Security Framework in SKK Migas Based on Integration of ISO 27000 and SABSA Model," in *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Jul. 2018, pp. 382–387.
- [14] J. Wu, Y. Wu, M. Yang, Z. Wu, and Y. Wang, "Vulnerability Detection of Android System in Fuzzing Cloud," in *2013 IEEE Sixth International Conference on Cloud Computing*, Jun. 2013, pp. 954–955, iSSN: 2159-6190.
- [15] C. A. Batista De Carvalho, M. F. De Castro, and R. M. De Castro Andrade, "Secure Cloud Storage Service for Detection of Security Violations," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, May 2017, pp. 715–718.
- [16] F. T. Waguie and F. Al-Turjman, "Artificial Intelligence for Edge Computing Security: A Survey," in *2022 International Conference on Artificial Intelligence in Everything (AIE)*, Aug. 2022, pp. 446–450.
- [17] K. A. Torkura and C. Meinel, "Towards Cloud-Aware Vulnerability Assessments," in *2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, Nov. 2015, pp. 746–751.
- [18] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-61r2, Aug. 2012. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- [19] N. I. o. S. a. Technology, "Security Requirements for Cryptographic Modules," U.S. Department of Commerce, Tech. Rep. Federal Information Processing Standard (FIPS) 140-2, Dec. 2002. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/140/2/final>
- [20] M. Ketel, "Enhancing BYOD Security Through SDN," in *South-eastCon 2018*, Apr. 2018, pp. 1–2, iSSN: 1558-058X.