International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Strengthening Data Security and Privacy Compliance at Organizations: A Strategic Approach to CCPA and Beyond

Shamnad Mohamed Shaffi

Colorado Technical University

Abstract: ***This paper presents a comprehensive strategy for ensuring compliance with the California Consumer Privacy Act (CCPA) and securing sensitive customer data within the organization. It focuses on evaluating and strengthening the current information security infrastructure, addressing potential risks, and enhancing privacy policies and training programs. The project aims to meet current and future state-level privacy compliance requirements while safeguarding Personal Identifiable Information (PII), Customer Proprietary Network Information (CPNI), and Payment Card Information (PCI). Key recommendations include risk assessments, the implementation of secure access controls, centralized data management, and network security measures. By adhering to established standards like NIST 800-30, the organization aims to mitigate risks, ensure regulatory compliance, and create a resilient data privacy framework that supports business growth and customer trust.***

Keywords: CCPA, data security, privacy compliance, risk assessment, information security, PII, CPNI, PCI, access control, network security, data privacy framework, regulatory compliance, NIST 800-30.

Project Outline and Requirements

CCPA Compliance Project Requirements

California Consumer Privacy Act is a compliance initiative to ensure the company provides new data privacy rights and disclosures to their employees and customers mandated by California law. Below are the high-level project goals:

- Enable enterprise to meet CCPA and other State's Privacy compliance requirements in the future- right to request not to sell the personal information, right to access personal information and request deletion, right to know about personal information in our care.
- Evaluate the security measures that are in place to help ensure organizations information is appropriately handled and protected.
- Analyzing the customer consent and preference management requirements and architect a centralized system that integrates Organizations' disparate systems.
- Updating organizations' internal and external privacy policies and training programs.

Introduction to Information Security

The management team want to do a thorough assessment on the organizations current information security infrastructure, processes and procedures in place to secure the sensitive and confidential customer information that is Personal Identification Information (PII), Customer proprietary network information (CPNI), and payment card information (PCI) to ensure the company is on compliance with the new data privacy law.

The Need for Information Security

Information security is very vital for the organizations to ensure that their critical and sensitive data such as customer information is secure and protected from threats and frauds. Organizations has legal obligations to protect the customer data privacy and confidentiality. Any treats or security instances like data breach could adversely affect the business and consequently the organization.

Potential Issues and Risks.

The company has operations on multiple lines of services and the enterprise data is not consolidated into a centralized data warehouse. Customer sensitive information could be saved in multiple applications in clear text format and this adds complexity and challenge in fetching the subscriber data to support the data request from customers. Understanding the inventory of records of all personal information used, stored, processed and transferred (processing activities) within Organizations applications, business processes, and third parties are critical to protecting the privacy and satisfying data subject rights.

Security Challenges of Allowing Consultants to Work On-Site

As part of the project, the company should focus on revisiting the internal and external privacy policies; creating new policies and training programs; establishing a data inventory and Record of Processing Activity (ROPA) and a privacy operating model.

A Review of the CCPA Compliance Requirements

CCPA will enable the enterprise to meet the other State's Privacy compliance requirements in the future and places Organizations in a legally defensible position for CCPA. It allows Organizations to know what personal information is collected and processed. The long-term benefit of this project is that it empowers Organizations to automate/utilize Record of Processing Activities (RoPA) data for privacy compliance requirements and beyond.

Security Assessment

Organizations management team decided to conduct a security risk process to identify, prioritize and estimate the organizations data assets and operations. The purpose of this activity is to help the security management team by identifying the relevant threats, internal and external vulnerabilities, weaknesses, and their impact to business and operations. The outcome of assessment will influence the countermeasures and strategies to secure the organizations

assets from any potential security risks. NIST 800-30 standards are being followed for the company's security risk assessment. The NIST 800-30 standards provides a step by step process for risk management for organizations on how to prepare and conduct risk assessment, how to update the key finding from risk assessment to required stakeholders, and how to develop a continuous monitoring process for identifying the risk before it happen.

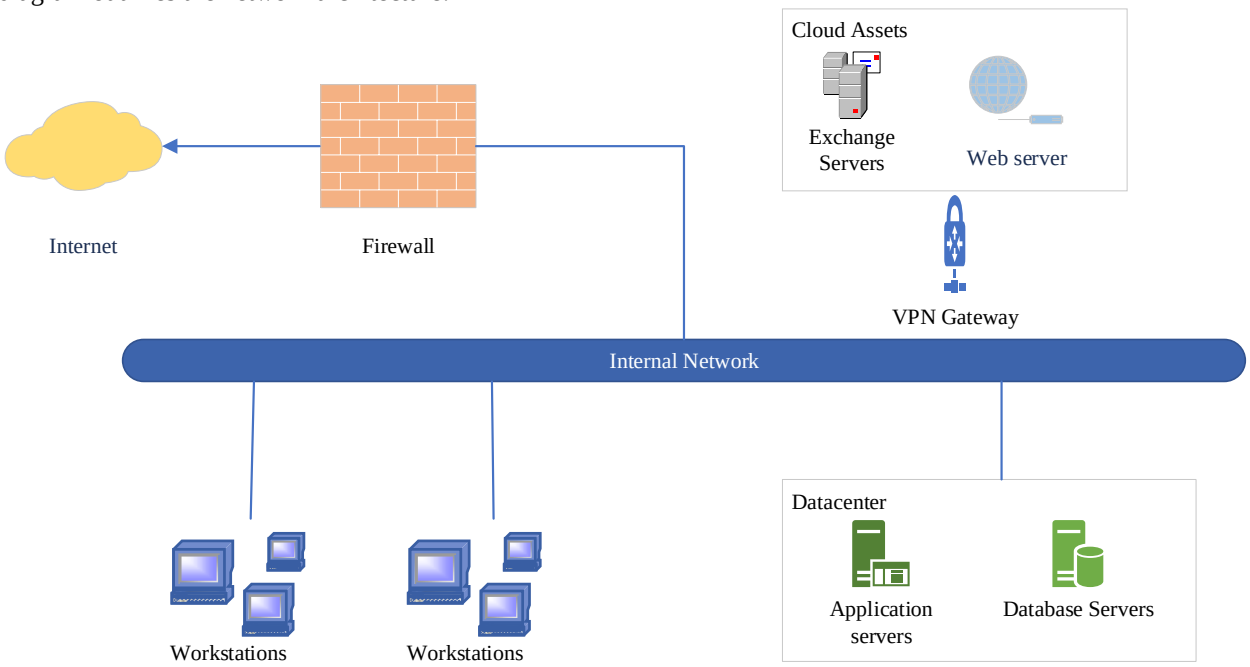
Current Assets

A list of enterprise application systems being used to run the day-to-day operations at Organizations.

Business Capability	System	Description
Customer Master Data	MDM	Stores master data of subscribers
Human resources Management	Workday	Stores company's employee data.
Supply Chain Management	SAP	Supply chain, inventory management, and order processing system
Billing Systems	Amdocs	Accounts payables, accounts receivables
Information Technology Management	Email Servers	Outlook application used to e-mail internal and external
Enterprise data services	Data warehouse	Reporting and data analytics
E-Commerce Management	Company website and Mobile applications	Web applications and mobile applications on public cloud.

Analysis of Current Network Topology and Risks

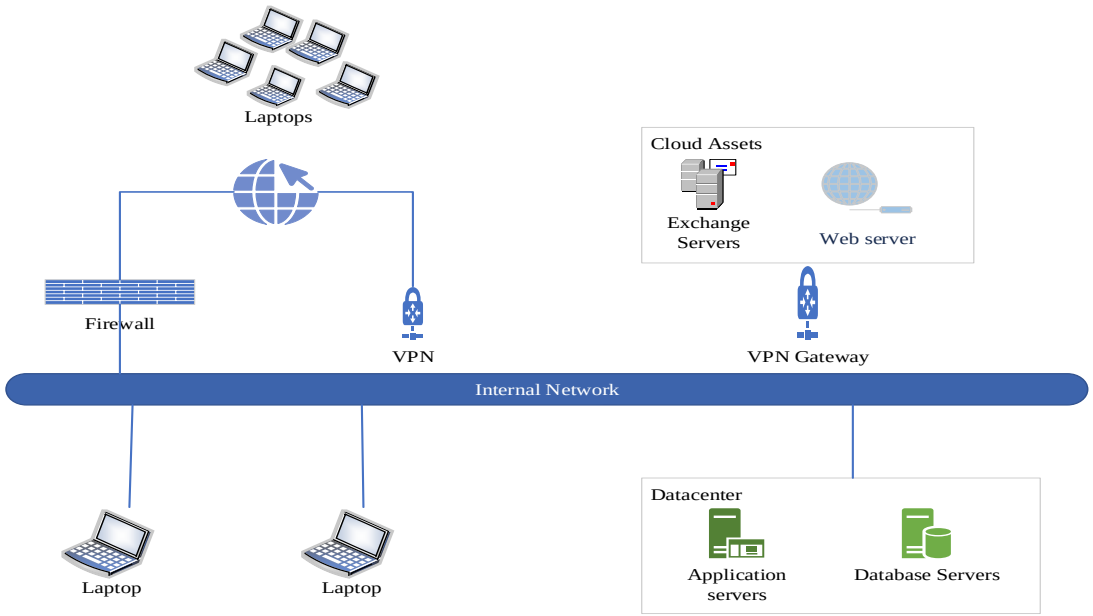
The diagram outlines the network architecture.



In the current network architecture of the datacenter hosting the application and database servers and the cloud assets are connected to the same network. The datacenter hosts the servers for SAP, Billing system, MDM and workday. The internet network connected to datacenter has only one firewall between the resources and public internet. Web servers and email exchange servers are hosted on a public cloud through a virtual private network. Below are the risks identified on the company's current network architecture.

System	Threats
Data center	• Since limited or shallow firewall security, it's possible for hackers to create fake access points and connect to datacenter. • Each access to hackers through internet
Applications on Cloud	• Potential risks of email and phishing spams. • Data loss without backups • Insecure APIs • Data breaches.
Desktops	• Antivirus problems • Unsecured USB devices • Redundant modems • Phishing threats

Below diagram shows network architecture after implementing new consultant network.

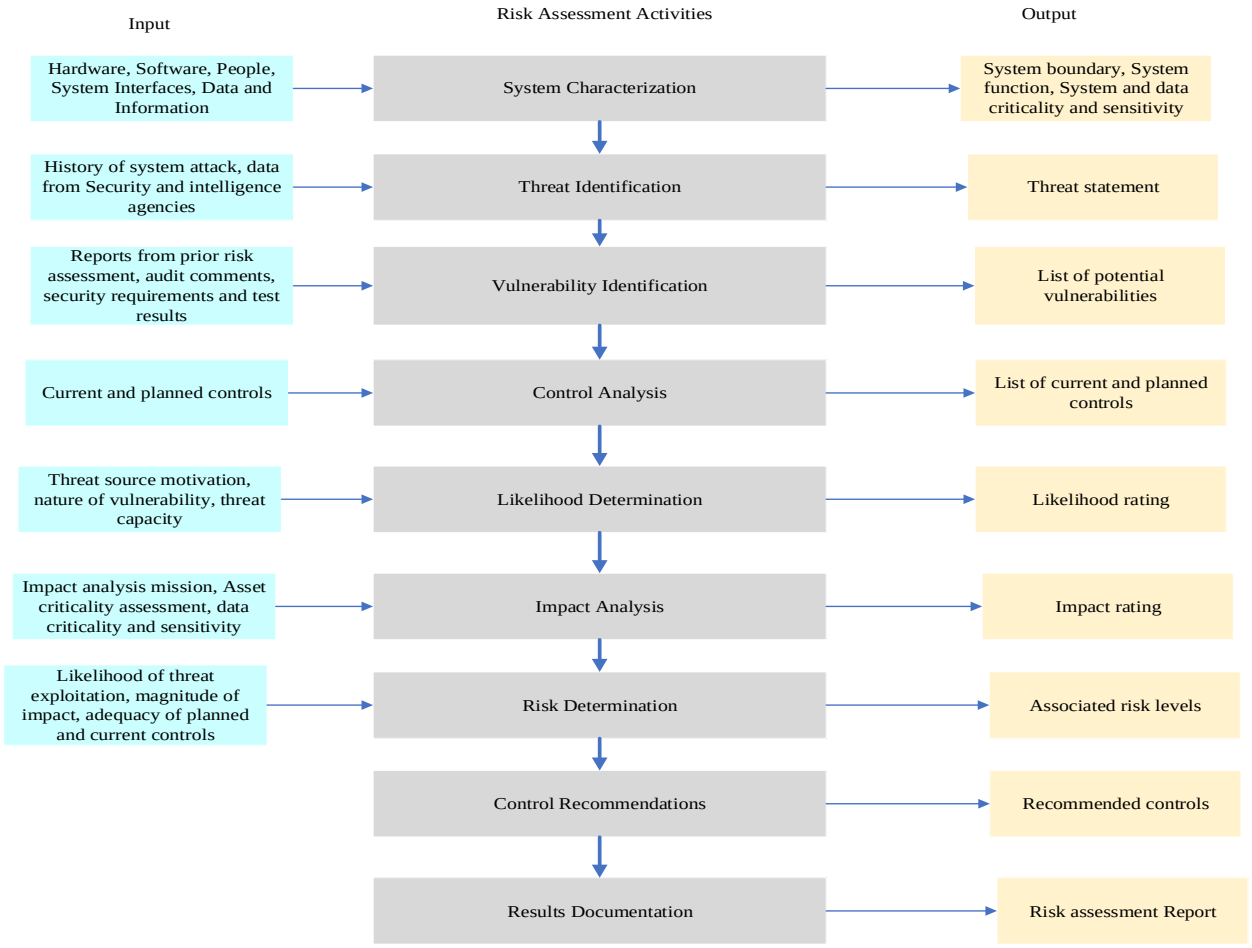


The new consultant network would introduce additional risks to organizations assets and resources.

- Lack of authority from organization to manage the laptops being used remotely and connected to company network through virtual private networks (VPN).
- Additional risk of malware from laptops through un-secured websites visited.
- Connecting the laptops to unsecured Wi-Fi networks can grant hackers access to VPN and organizations assets and sensitive data.
- Risk of remote laptops are not being scanned for viruses and malware.

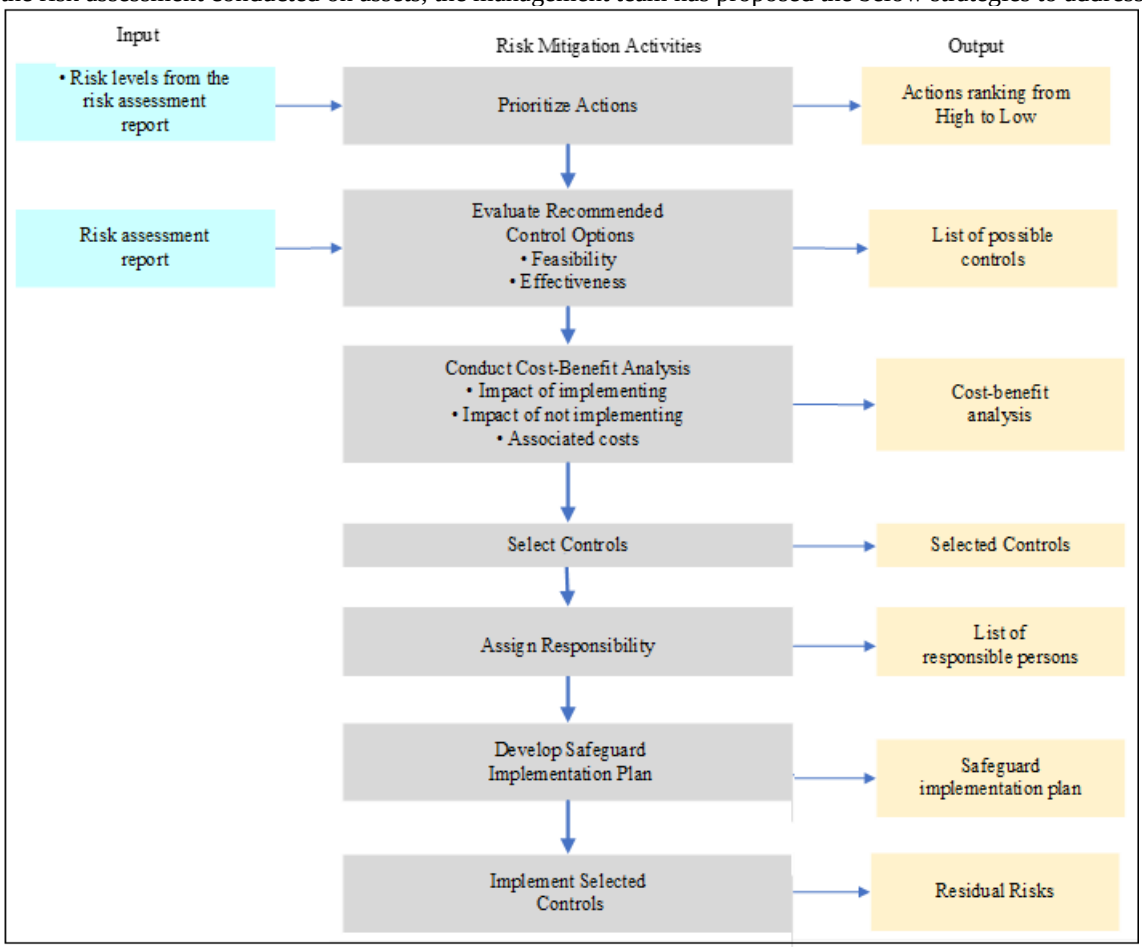
Risk Assessment Methodology

Organizations conduct risk assessment as the first phase in the risk management process. The objective of the assessment is to understand the extend of the potential threat and its risk and impacts on the organization's asset and business. The nine steps from the NIST standards for the risk assessment methodology are shown below.



Risk Mitigation Methodology

Based on the risk assessment conducted on assets, the management team has proposed the below strategies to address the risks.



Access Controls and Security Mechanisms

The Organization has many software applications to run their daily operations and business. Each of these applications is hosted on different platforms and hence has different user authentication processes and procedures. The security management team has assessed the existing access controls and recommended implementing the below access control and security mechanisms.

- Active directory service for all users, groups, and roles.
- Single sign-on for cloud users.
- Provide secure VPN access for remote users.

Access Controls of Existing Applications

The following are the access control measures recommended for existing applications.

Business Capability	System	Access Control Mechanism
Customer Master Data	MDM	Single sign-on for authentication and active directory for authorization
Human resources Management	Workday	Single sign-on for authentication and active directory for authorization
Supply Chain Management	SAP	Supply chain, inventory management, and order processing system
Billing Systems	Amdocs	Active Directory and single sign-on (Role based access) with additional SOX compliance controls.
Information Technology Management	Email Servers	Active Directory
Enterprise data services	Data warehouse	Active Directory and single sign-on (Role-based access)
E-Commerce Management	Company website and Mobile applications	AWS Directory Services

As the company is providing laptops to employees to connect remotely in addition to existing workstations are office its recommended to have a centralized login through active directory. It's also recommended using any Network access control (NAC) providers to support access management on devices. A few benefits of using a NAC provider are the following.

- Centralized login to workstations and laptops.
- Reduces threats by enforcing security and antivirus policies.
- Integration with Active Directory and allows personnel to perform only role-based jobs.
- Continuous vulnerability assessment and remediation.
- Protect unauthorized access, threats, and malware
- Keep track of profiles and software inventory in each workstation.

Network Authentication Schemes

Single Sign-On

Identify and access management (IAM) is a framework of policies and technologies that ensures that the person has the right access to enterprise technology resources. Single sign-on (SSO) is a property of IAM that allows users to use a single set of credentials to login and authenticate with multiple applications. These facilities a single access process to multiple resources connected to an enterprise's local network. SSO provides the benefits of avoiding the credential re-authentication and reducing the application admins efforts, it increases compliances through a centralized repository and helps in producing detailed user access reporting.

From the Organizations point of view, single sign-on is a very important productivity and security enablers. The recommendation is to use single sign-on services like Okta integrated with AWS directory services for their employees to authorize and authenticate to login to the billing system, MDM, Workday, and SAP. Enabling multifactor authentication will provide additional security along with a single sign-on.

Virtual Private Networks

Employees connect to the company's internet network using Virtual Private Networks(VPN). The VPN should be integrated with active directory services. The following are a few benefits of using a VPN solution in the enterprise.

- Allows employees to connect with the company's internal network.
- Helps admins to track the profile and system configurations to ensure that the device is safe from threats, viruses, and malware.
- VPNs are compatible with different platforms.
- Affordable.
- Data transfer will be secure and protected.

There a few disadvantages of using VPN such as performance issues while connecting remotely, added costs, legal policies that a few enterprises don't allow to connect to their internal network from outside, difficult in the initial set-up for business users, etc.

The laptops provided by Organizations would be provisioned with a VPN Client software like Cisco AnyConnect. Employees are required to login to VPN Server using Active Directory login. It's also recommended to enable multifactor authentication for VPN access as well.

Software and Database Security

Security Policies, Procedures, and Regulatory Compliance

As Organizations is planning to implement IPO, it's important to prepare effective and efficient security policies and processes and a robust audit control mechanism.

Regulatory Requirements of Sarbanes-Oxley

The Sarbanes-Oxley (SOX) Act was introduced in 2002. The objective of the law was to introduce major reforms to existing auditing and financial compliance reporting and protect the organizations from fraudulent practices. It was intended to protect the public and investors by requiring the reliability and accuracy of financial disclosures. The law enforces strict security controls and audit processes with the enterprise information data. The following are the key requirements for Sarbanes-Oxley (SOX) compliance that should be considered.

- Implement a strict audit trail of access to enterprise applications mainly the financial systems of records.
- Ensure to produce control reports to the auditing team as proof of having adequate controls are in place for financial data.
- Robust applications to manage employee data, their benefits, and other expenses.
- Ensure IT platforms that handle financial data has secure and protected.
- Continuous monitoring and reporting on security policies and mechanisms.
- Inform SOX auditors on any security breach incidents and their impacts.

Security Policies

Information security policies establish the rules where organizations can direct funding, people, processes, and technology in a retable and secure manner. Information security policies are developed by examining compliance requirements, obligations under the law, and organization-wide policies and practices. The information security program policy includes the program purpose, program scope, addresses compliance requirements, and assigns who is responsible for the information security program. The following are the security policies recommended.

Policy	Description
Acceptable Use Policy	Provides guidelines for employees, privacy and security expectations, data retention, and employment hire and separation.
Operational policy	Policy provides guidance for specific policy areas at an organizational level
System-specific policy	Policy provides guidance around how a specific information system should be operated and maintained
Change management policy	Provides processes and guidelines to be followed for implementing a change within the enterprise.
Data Security policy	Ensure proper data classification guidelines and mechanisms to protect the sensitive and restricted data.
Physical Security Policy	Ensuring the guidelines on physical security on the office premises.
Consent and communication policy	Ensure that different disclosures, personnel consent are as per compliances.

Security Policy Controls

The systems and protection policy establish the rules necessary to properly establish network segmentation and boundary protection thought the organization, as well as establishing the necessary rules around how cryptography will be implemented.

Policy	Control
Acceptable Use Policy	Monitoring, controlling, and protecting organizational
Information Asset management Policy	Employing encrypted design patterns, and software development methods.
Acceptable Use Policy	Implementing subnetworks for remote workstations that are physically separated from internal networks
Acceptable Use Policy	Implementing mechanisms to prevent unauthorized disclosure of information.
Acceptable Use Policy	Terminating network connections associated with communication sessions at the end of the sessions or inactivity
Information Asset management Policy	Employing cryptography to protect the confidentiality of system information
Acceptable Use Policy	Controlling and monitoring the use of mobile codes
Information Asset management Policy	Protecting the confidentiality of information at rest
Physical Security Policy	Ensuring visitor management processes

Data Protection

Data at Rest

For data at rest its recommended to implement a tool such as BitLocker on a Microsoft Windows system. This tool serves to ensure that data on a hard drive is kept confidential if the hard disk is stolen. Storing the information at different locations can decrease the likelihood of hackers gaining access to complete information to commit fraud or data breach incidents. Data that resides on cloud storage should be encrypted when stored to ensure that the data cannot be removed

Data in Motion

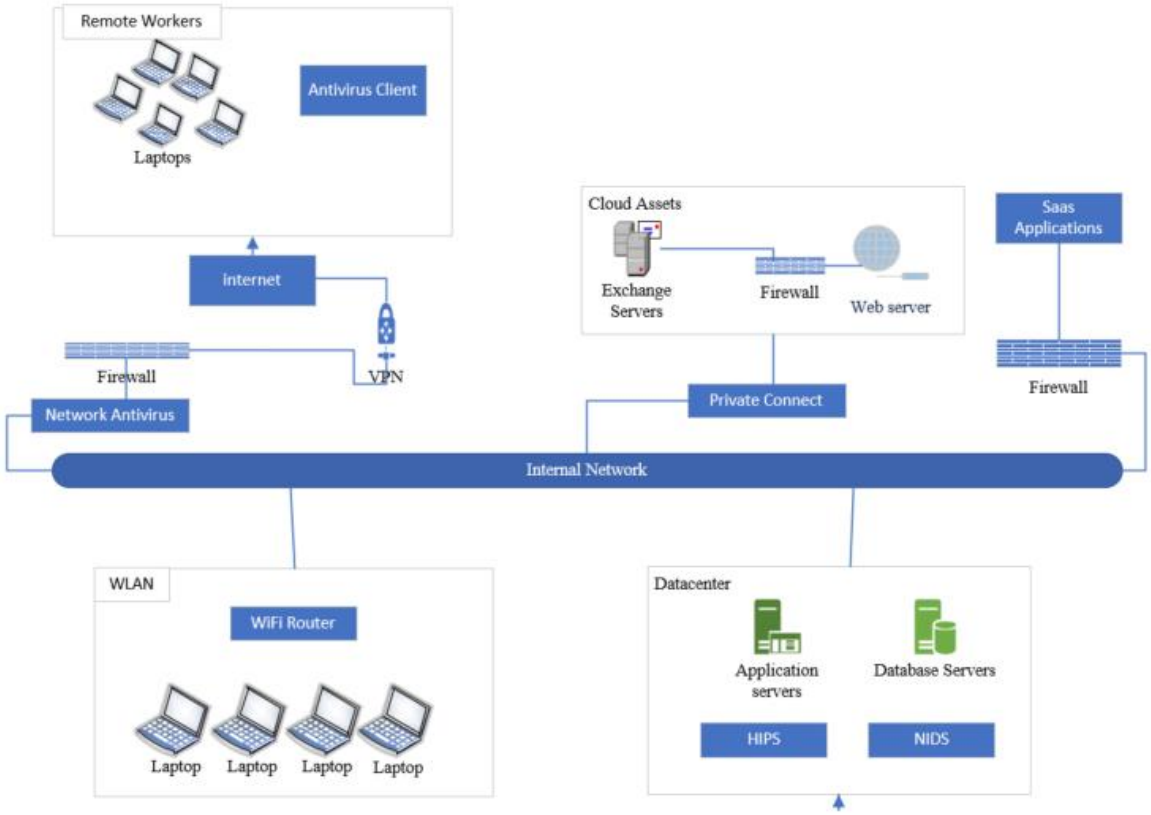
For data in motion its secure to implement a protocol such as IPSec to protect data being transmitted from one server to another. Encryption should be used when data is moved inside and outside of the cloud. As data in motion is vulnerable to threats and attacks, a robust process and mechanisms should be in place to secure the data asset, such as using an encrypted platform while sending sensitive or confidential messages.

Network Security

Based on the assessment conducted, the following changes are proposed to Securely configure the network hardware and configurations will ensure that to have an effective and secure communication infrastructure.

- Network infrastructure must be designed, implemented and operated in a manner consistent with company policy documents.
- Only authorized users and systems with legitimate need are eligible to access network systems and devices. All User IDs must meet authentication requirements and must be approved and audited by designated network and/or security personnel.
- Only authorized users must be permitted to make changes to or install network components on company's networks.
- Operational responsibility for network infrastructure must be segregated from computer system administration where appropriate.
- Network diagrams must be maintained and kept current by network management teams, using automated network discovery tools where possible, and should be reviewed annually by the asset owner.
- Ports that are not required for business purposes must be disabled and protected against misuse.
- A On-prem and on cloud network architecture needs to be implemented.
- Implement Intrusion detection and prevention systems.
- Implement network firewalls.
- PCI in-scope firewalls and routers must be reviewed at least every six months. b. Non-PCI firewalls rules must be reviewed at least annually, and any unnecessary rules must be removed. c. Other network devices will be reviewed on a regular basis.
- Networks must be segregated into functional groups of services, user access, and information systems. Segments with a different need of protection must be divided into separate security zones or domains. ii. The division into security zones and selection of security requirements must be performed based on a risk assessment. For e.g., gateways to external networks and between security zones must be protected.
- Traffic monitoring for inbound and outbound messages.
- Enable multifactor authentication.
- Establish a guest network on the wireless infrastructure for visiting customers and business partners.
- Enable strong encryption on the wireless infrastructure.
- Enable a mobile device policy.
- All network devices must be discoverable and tracked by a centralized management and monitoring system.
- Third-party connections must be reviewed, audited, monitored and logged appropriately.
- Firewall rules not in compliance with the above requirements must have a DSO approved exception.
- Network intrusion and monitoring systems must identify and alert CIRT personnel to suspected compromises.

Considering all the factors, the revised network topology is recommended as outlined in below diagram.



Protecting Data

The Intrusion detection and prevention tools allow the incident responder to have visibility into the network, allowing them to establish a baseline for what it normally looks like, and to easily visualize when anomalous behavior is occurring.

Intrusion Detection Systems (IDS)

An IDS tool needs to be in place to perform real-time monitoring of network and server/workstation activity. These tools are typically signature-based and look for suspicious activity that matches a preconfigured signature. If a condition matches a signature the tool will either block (IPS) or alert (IDS). The Advanced Intrusion Detection Environment(AIDE), Snort (from Cisco systems), Snort, Fail2Ban are a few IDW systems available in the market now. There are two types of intrusion detection systems –

- Network intrusion detection system to detect malicious activities at the network layers
- Host intrusion detection system to deployed on a host application that could monitor and help detect malicious activities on the business-critical servers. Each host application is required to install software on it, but it is very typical to install the HIDS on every device connected to the network.

Intrusion Prevention Systems (IPS)

Organizations need to deploy IPS appliances at network ingress locations on the network. Pluck, OSSEC, Zeek, Open WIPS-NG are a few IPS tools used across the industry. IPS systems can prevent any threats to applications on the network such as phishing, spear-phishing, etc. hackers target the systems on different methods like installing software, set-up user account to get access to a network, databases, and applications. Signature-based detection and anomaly-based detection are two types of IPS systems. The signature-based detection method detects the patterns in data to identify any threats, and anomaly-based detection tracks unusual activities on the network. The IPS systems provide the following capabilities:

- Provide proactive, in-line network protection against network threats including DOS attacks, worms, spyware, Trojans and viruses.
- Security updates from the Digital Vaccine Service, ensuring current protection against emerging threats.
- Monitored 24x7 by a third party.

References

[1] Cisco. (n.d.). *What is network access control.* Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

[2] Davis, S. (2019). *Why Your Business Needs Network Access Control.* Retrieved from https://www.tedsystems.com/why-your-business-needs-network-access-control/

[3] Death, D. (2017). *Information Security Handbook: Information and Data Security.* Birmingham UK: Packt Publishing Ltd.

[4] Harris, S., & Maymi, F. (2018). *CISSP All-in-One Exam Guide.* New York: McGraw-Hill.

[5] Korolov, M. (2019). *California Consumer Privacy Act (CCPA): What you need to know to be compliant.* Retrieved from https://www.csoonline.com/article/3292578/california-

consumer-privacy-act-what-you-need-to-know-to-be-compliant.html

[6] Morrison, S. (2019). *California's new privacy law, explained.* Retrieved from https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained

[7] *Sox 101*. (n.d.). Retrieved from https://www.sarbanes-oxley-101.com

[8] Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* Retrieved from Risk Management Guide for Information Technology Systems: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf