Session: 202130

Charles Sturt University

Cloud Computing

Assessment No.4

Cloud Proposal and Design

Case study

Submitted by:

Johan Sebastian Ramirez Vallejo

Contents

Figures Table

1. Proposed Web and IoT Design Architecture for the Cloud

1.1 Suggested architecture.

The issues are founded on the administration of **computing**, **storage and networking** which concern **High availability (redundancy)**, **security**, **operation** and **management** that are necessary for business continuity. Cloud provides tools that support the operation and help to keep all according to the plan.

Key issues affect the 3 important capabilities of the system confidentiality, integrity, and availability. computing issues are related to lifecycle management such as monitoring and maintenance. Therefore, security issues are related to technical, procedures and operation. Storage issues are related backup process that is not appropriate to a DR. Infrastructure is poor which DR alarms need investment to move to the cloud.

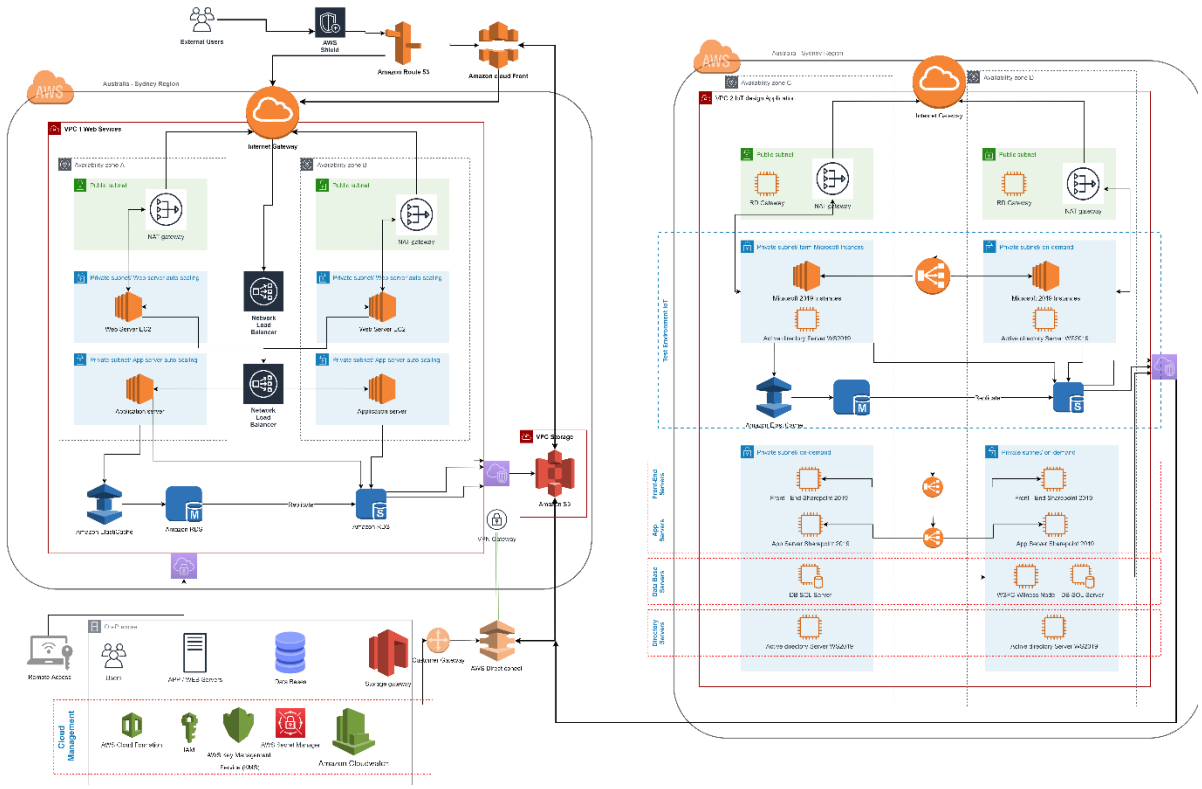

Figure 1. Suggested Architecture

This suggested architecture follows the best practices to move to the cloud and respond how improve DR alarms according to a high availability hybrid deployment. It follows resilience patterns supporting DR. It is important understand the roles in the governance of the cloud to obtain the best performance. The architecture is base in the 5 pillars of the AWS-well-Architecture Framework (Amazon Web Services, 2021i) which are Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization.

Data sovereignty for DR alarms is very important for their designs and intellectual property. The cloud is set up in Sydney Australia in 4 availability zones that convey in hybrid deployment to make available and secure. The connectivity is recommendable use AWS direct connect for a unique canal to his cloud between them.

1.1.1 Web services architecture deployment

The web services architecture deployment suggested architecture provides a secure environment for customers and Users in Dr alarms. It is a three-tier model where it is separate into presentation, application, and persistence layers for data(Amazon Web Services, 2019b). Therefore, it is a hybrid deployment (Amazon Web Services, 2020b)where sensitive data is store on-premises to increase security for the data that DR alarms manipulate. Scalability is provided for each layer presentation and application. Thus, it is performance, failover, and availability for data is providing resilience against to any catastrophe. To get the best approach of this architecture the peak of traffic is required to be analyse and set up to provide a beneficial cost through the correct auto-deployment when it is required.

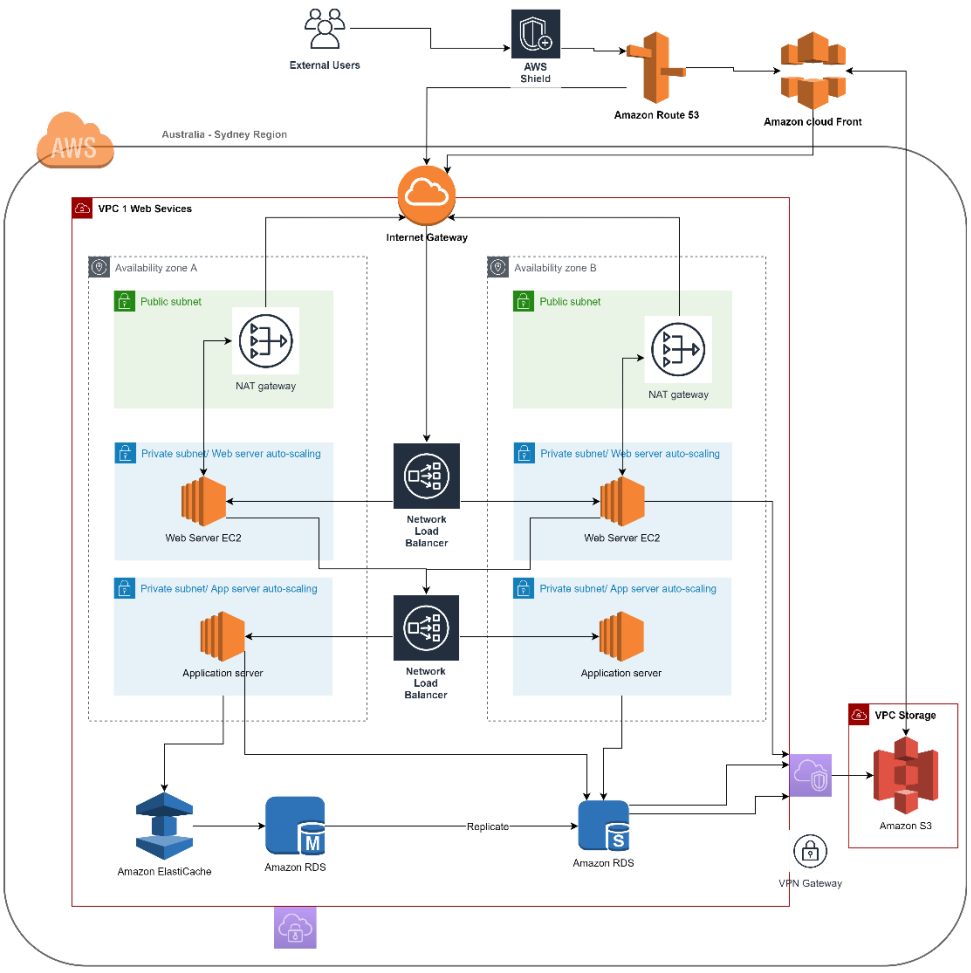

Figure 2. Web Hosting Architecture multiple layers

1.1.2 IoT Design application deployment

The suggested architecture provides a IaaS manageable and secure environment for user in DR alarms. There are 2 private subnets to separate and secure the data between them. The fist private subnet contains a scalable and resilience farm instances with the availability to allow users to test security IoT application(Amazon Web Services, 2019a). The second private subnet contain the highly availability, auto scalable and resilience SharePoint architecture for the business workflow demand changed. This private subnet follows 4 layers which are presentation, application, persistence data, and control (which is an extinction of and domain control from on-premises domain control)(Amazon Web Services, 2020c). The entire IoT Design architecture allows a secure remote control through to RD gateway encrypting the data in transit for remote administration. Each component will be explained below.

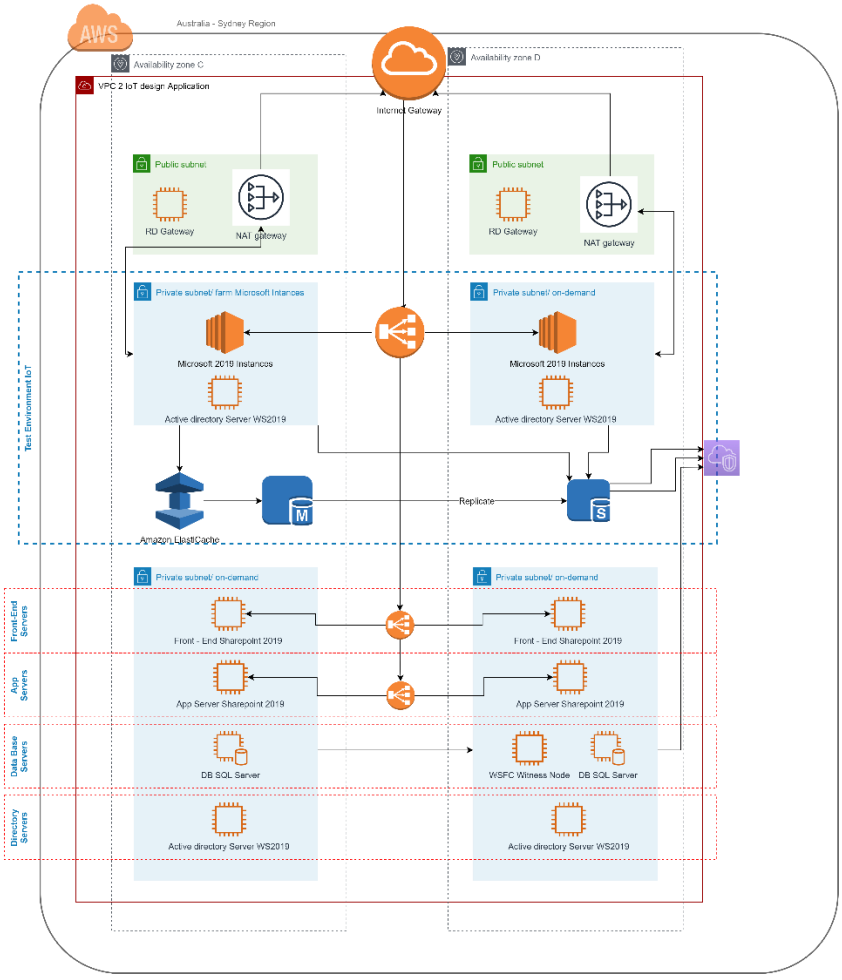

Figure 3. Windows environment, and windows SharePoint architect model

1.1.3 Architecture components

Each of the following elements have different purposes that all combined provide a well design architecture sticky to the 5 pillars framework.

Cloud Management

AWS CloudFormation: automate best practices in the cloud, creating the model collection of the resources under your control (Amazon Web Services, 2021d).

AWS Key Management Service (AWS KMS): is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications (Amazon Web Services, 2021g).

AWS IAM: AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely (Amazon Web Services, 2021f).

AWS Secrets Manager: extra layer to protect the IoT design application. It is combine with IAM roles (Amazon Web Services, 2021h).

AWS CloudWatch: is for monitoring and observability. Provides data of the applications respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health (Amazon Web Services, 2021e)

Figure 4. Management Tools

Infrastructure Security

To increase the security in the architecture should follow the best practices for configuration and protect the instances and data in transit and Rest. This is archivable setting security groups and encrypting in and out data. It is also important for data bases AWS automatically patches and make backups. The architecture uses a replication model including mirroring for read-only copies and log shipping for always-ready passive slaves.

1. **Internet Gateway:** it the door of the VPC to the internet and the controls must be against this door (Amazon Web Services, 2021l).
2. **Network Load Balancers (ELB)*5:** they allow the scalability on demand and resilience (Amazon Web Services, 2021k).
3. **NAT Gateway:** allow to connect to internet from instances in private network. Increasing the security (Amazon Web Services, 2021m).
4. **Amazon ElastiCache:** it the cache for the layer application reducing latency(Amazon Web Services, 2021a).
5. **Manage Database RDS:** the configuration of RDS allows resilience to catastrophes. Its high available(Amazon Web Services, 2019b).

6. **VPN Gateway:** allow to encrypt access and data in transit.
7. **AWS Direct Connect:** is a secure canal between the company and cloud provider.
8. **Storage gateway:** allows the hybrid environment for data storage in cloud.
9. **Remote Desktop Gateway:** establish a secure, encrypted connection between remote users and EC2 instances running Microsoft Windows(Amazon Web Services, 2019a).

Vulnerability reduce

Every time advance the techniques to provide attacks such DDoS, and the services above and the load balancers allow to respond to the attack scaling the resources to keep the services running.

1. **Amazon route 53:** is a highly available and scalable cloud Domain Name System (DNS) web service(Amazon Web Services, 2021b).
2. **Amazon Cloud front:** is Fast, highly secure, and programmable content delivery network (CDN). Combined with route 53 and AWS shield. It is a extra layer against attacks(Amazon Web Services, 2019b).
3. **DDoS Protection with AWS Shield:** it is extra measure against DDoS attacks. It helps safeguards applications running on AWS(Amazon Web Services, 2020a).

Benefits:

- The responsible configuration and scalability allow respond to increasing traffic.
- Failover configuration allows accessibility to secure data.
- Encryption inbound and outbound protect data on-premises and cloud.
- Configuration of security groups NACLs for each instance allows an individual protection as a firewall that allows enforce the model.
- Cost-Efficiency if is known the peak periods.
- Different layers for application resilience.
- Low latency for workloads
- Billing optimization
-

Critical Points:

- In response of DDoS attacks the scalability can go up and increase the costs to keep and service.
- Require strict security control.
- Constant auditing.
- Require constant training.
- Keep connection between private and public clouds

Issues:

- Deployment knowledge.
- Investing time increasing security behaviours.
- Bandwidth for DR.
- Secure Internet Connection can increase the cost.
- Control location sensitive data increase complexity.
- Compatibility between on-premises and cloud
- Keep integration between data and application.
- Data synchronization

1.1.4 How to improve data center On-premises?

Computing environment, Network and Power

It is necessary solve network problems on - premises to ensure a secure connection and highly available. First, it is suggested the connection should be connected through two ISPs with two routers in redundancy a firewall to protect the data from the internet (Erl et al., 2013) . Electrical system should be redundant and maintainable without impact (Amazon Web Services, 2016). UPS provide power backup if something occur. The environment for a datacenter need two important things the correct climate and fire protection which are also recommended (Amazon Web Services, 2016). Location and safeguard the computing in a safe place with the correct conditions is highly important for the business continuity. The next image shows the logic behind network configuration.

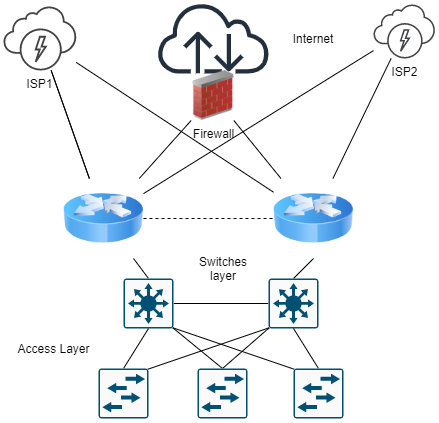

Figure 5. On-premises network configuration

Computation

Independently of the solution that the client chooses there is a certain responsibility by part of the client to maintenance their computing, although the solution reduces compute to manage the maintenance on premises is part of the costumer. It is highly recommended because the solution will focus on sensitive data storage on premises. The security controls are needed there too such as accounts, credentials, and segregation of duties just like it is done in the cloud managing IAM.

Security

The most important to DR Alarms is its sensitive data. So, it is recommended to isolate the data center and apply security protocols and polices. Provide training to IT administrators and employees about the cloud and security because it has been evidenced that most cases of hacking are the fault of the users. In addition, it was also found that in the data center there is no proxy server and no antivirus which it is recommended that it be installed and established.

2. Threat and Risk Assessment report for services and data in the Cloud

Considering the new Dr alarms strategy of moving web services to the cloud in order to increase scalability as well as the flexibility to deliver their services to customers and internal users. This movement provide to the company less control over their resources and increase the risks because internet is a big place where many people want access to information to trade with it. Therefore, the mayor risk is security over the data that the company collect from their costumer and transport to premises. To reduce the risk, it is necessary to restrict the access, create protection protocols, create redundancy and monitoring to guarantee the integrity, confidentiality, and availability. It is also important that the company provide compliance to the internet regulations. So, it is important the company locate their services where are located (Australia) to meet the compliance requirement.

The company is moving the web services and their environment for IoT design application, so, their mayor risks are related to attacks to take down the services, stole data, vandalizing content and unauthorize access.

Aws shared responsibility model is a tool for costumers to support them to archive security objectives. The company have be familiar with this to build a secure solution and applications on top of the services AWS operates, manage and control (Amazon Web Services, 2019a).

To identify the potential threats to the system and determine the risk. To reduce the risk during and after migration. Determining this allows to create a set of controls which are related to the privileges who are authorized to access to AWS management console to perform job task.

2.1 Risk identification

Data is the most important for every organization. Dr Alarms has been experiencing multiple cyberattacks, compromising their private and customer data. The poor procedures of maintaining and internal access control lead security problems. Considering the behave of the company in multiple aspects the risk is high according to the security in the cloud. Leak knowledge about the cloud increment more the risk of every service that the company have in the cloud (Justyna Kucharczak & Inc, 2020). The risks will be categorized between 1 to 3 where 3 there is more likelihood to happened. Controls will be addressed through different methods and techniques to reduce de risks.

2.1.1 On-premises Risks

- **Attack surface:** set of exploitable vulnerabilities in customer environment.
    - **Affect**: network, software, and users (administrators and user with access to the AWS management console)
    - **Control**: Reducing the number of ports accessing to the network, and source network or IP address.
    - **Likelihood and Impact** :2-High

2.1.2 Physical Risks

- **Access to physical provider resources:** Personnel from provider can access to physical infrastructure.
    - **Affect:** Physical network, resources, customer services, cost
    - **Control:** every services provider has to warranty that they cannot access through Service level agreement SLA
    - **Likelihood and impact:** 1-High

2.1.3 Services Risks

- **Attack tenant:** multiple tenants are in the same space. So, the risk that other tenants can be affected by those attacks.
    - **Affect**: integrity and confidentiality of the costumer services
    - **Control**: locate the services in private subnets, set up correctly security groups, NACLs.

  - **Likelihood and impact:** 3-High (attacks occur all the time)
- **Hypervisor attacks**: the hypervisor is a piece of software that provide control of physical resources if this code face attack provide malfunction of this control
  - **Affect**: malfunction of the services located in each VM.
  - **Control:** Provider polices – SLA – Monitoring - Auditing
  - **Likelihood and impact:** 1-Medium
- **Data disposal**: Provider provide to customers a tenant space which provider must be sure to clean for the next tenant and make sure the data do not overlap and expose for the next tenant. This can occur during the migration to the cloud, Scaling up and down the storage.
  - **Affect**: data integrity and confidentiality. Important data can be expose could be sensitive data, intellectual property, and application code.
  - **Control**: Service level Agreement SLA Provider must warranty.
  - **Likelihood and impact:** 1-High
- **Misconfigurations - Changes unauthorized:** Staff that requires access to the management console provide changes. To a service works in the cloud require basic configurations even for APIs. But, for security purposes requires follow different methods, policies, configuration techniques and best practices to work properly and safe.
  - **Affect:** integrity, confidentiality, availability – Services
  - **Control:** IAM – PAM controls use Multi-Factor Authentication (MFA) - AWS Key Management Service (AWS KMS) encrypt the root of domain controller. To avoid misconfigurations must follow the best practices to increase security in different places in the architecture (Management, different layer in the logic network (security groups, NACLs, load balancer, route tables), server configurations). Control Patching logs - Changes controls logs – Antivirus on domain controllers. Monitoring (automatic activities looking for vulnerabilities, test for direct vulnerabilities and notifications to immediate respond) and Auditing activities, training to staff who have access.
  - **Likelihood and impact:** 2-Medium (Attacks such us Insider Threats from former employees)

- **Access unauthorized:** The cloud environment works essentially with and Access management. Once an attacker obtain access to management console, have access to all sensitive data.
    - **Affect:** integrity, confidentiality, availability – Services- business disruption - elimination of data, capabilities, assets such as intellectual property. The reputation and financial bottom line. DR alarms works with sensitive data from governmental institutions the effect and consequences are mayor. It can affect third party and face demands for it.
    - **Control:** stress IAM-PAM controls, secure and rotate password of management keys, databases passwords. Automatic activities and notifications to keep this control. Eliminate unused accounts, Monitoring for activities and auditing controls. Encrypt data in transit and in REST is the best practice. Backup and Disaster Recovery is required and AWS services like Amazon S3 APIs, AWS Storage Gateway, AWS Backup, AWS Data Sync and AWS Transfer for SFTP enable to implement a disaster recovery strategy data hosted on-premises (Amazon Web Services, 2020b). Use AWS services for avoid exploit attacks such us AWS Route 53, AWS WAF, AWS CloudFront Security controls on-premises to increase security activities.
    - **Likelihood and impact:** 2-High (Attacks occur all the time. Data breach, account Hijacking, looking for credential occur all time)

- **DDoS attacks:** They are attacks that attempt against availability that frequently make requests to the servers to try to get down the service.
    - **Affect:** The cost due to that the architecture is built to auto-scale and the constant request tell the load balancer that need increase resources that cost.
    - **Control:** AWS shield is a service that detect this attack and protect layer 3,4 and 7 OSI model. It is a service supported 24*7 by amazon. Monitoring (notifications to immediate respond) and Auditing activities.
    - **Likelihood and impact:** 3-High (Attacks occur all the time. Data breach, account Hijacking, looking for credential occur all time)

The protection of data and runtime of DR alarms is highly concerned for their customers. The trust in security should deploy in all surfaces either on-premises or cloud. The risk assessment is an essential tool see what the risks are during and after of migration. To put on control and strategies to reduce the risks. The security is a shared responsibility where DR alarms must be increase to extend their business(Amazon Web Services, 2021n). The architecture best practices must be put in place to develop a secure environment for services in the cloud.

3. Proposed IoT Design Security controls for the Cloud

Dr Alarms is developing a IoT monitor device which support organisations' network monitor activities. It is a big opportunity, but it also brings security, risks, and privacy concerns. Therefore, the protection of their costumers is their high priority where IoT devices have to start and end with security (Amazon Web Services, 2021o). Like a cloud solution where the protection is through multi-layers of rules, controls, monitoring, and auditing follow best practices framework, same occur in the edge of the cloud where the exchange of sensitive and personal data must be protected, and they have a potential impact of data sovereignty.

Dr alarms is expanding internationally, laws and regulations can vary around the globe. MD wants that IoT design data holds in Australia this is concerns to protect the intellectual property of the product when they turn to the cloud. So, Data protection authorities (DPAs) look closely where the data collected ultimately is processed. Thus, regulatory obligations are subject to jurisdictions that are required to meet wherever possible. So, it is important to implement controls to comply to them. Intellectual property also need protection, and this can be archive through different tactics and controls that combined can make strong the protection of IP (Commission, 2021).

Securing IoT devices should be considered at the development earlier stages. It also important that the development conserve the development lifecycle and secure the collection of data with encryption in Transit and in Rest. The architecture suggested support this practice to archive IP security and data sovereignty.

3.1 Intellectual property (IP) protection

The protection of Intellectual property translate into the protection of IoT designs and everything that it involved. Software, app architecture design, physical designs etc. All of this must be protected from different fronts: regulations, standards, hackers, staff inside of organization, former employers, contractors, customers, and data transport in different layers. So, a combination of different good practices, business tactics and methods are keys to archive IP security. Understand deeply the risks, take technical considerations, take advantage in the compliance, develop agreements and have a data breach policy are the

main aspects to have a security environment to protect the IP (Cidon, 2015). The next steps were divided in 3 areas in pro of confidentiality, integrity, and availability to face the risks.

3.1.1 Protection by law (Legal and regulatory controls)

It is well known if it is created something, it is necessary run to patent and get protection by law(Commission, 2021). But there are more laws thar relevant here:

Dr Alarms is a company that holds in Australia. Therefore, the laws covered them. The laws that must concern and cover them are:

Patent protection

Obtain the patents of the invention is the most assertive step to protect the designs, products even process that meet certain specifications. Apply for a global patent could result beneficial to business strategy.

Trademark protection

Every company and products have a name which is how they are represented in the market. So, register the mark or brand is assertive to get protection by law.

Design protection

Australia has the registration design framework which protect the design by legislation. This also support protection.

3.1.2 Management of information (procedure controls)

Control the information across the company is one of the most important practices that the company need to adopt. The mayor of breaches occurs inside the companies or from former employers. For that reason, increase security, stablish preventive, detective, corrective controls, and determinate activities such as monitoring and auditing proposes one step more to adopt toward security.

Trade Secret

Hold information inside of the company can be difficult even by stakeholders but identifying what is top secret can be manageable through limited people.

To make strong this Signed Proprietary Information & Inventions Agreements by All Employees and Contractors support to keep the secret across the company. This agreement also should cover employers that leave the company (Lord, 2020).

Non-Disclosure Agreements with Customers

The agreements are the best way to obtain confidentiality. Keeping clear this in DR alarms SLA for IoT devices services support the security.

Security behaviour

Security awareness and training is important to archive security. Polices of remote use, phone use, workstation use etc. support the control in the organization. But this is not just applying to secure IoT designs, this also applies to everything inside of the organization. incident response processes help for quick risks reduction. Management oversight through Monitoring and auditing for personnel who handle critical systems.

3.1.3 Data protection (technical controls)

Data it is the major concern by organization, but the intellectual property data is the backbone of it. Above concern more to the managers but the next security practices concern to the configuration to IT administrators and controls that they need to do to protect the IP.

Access to Proprietary Information

Apply authentication and access control mechanisms where is proprietary information is located. Dr alarm IoT cloud will use a SharePoint software to increase the experience. So, provide training to work security in this environment and enforce resource consumption limits and throttling to protect the availability of shared resources hence the goal.

Encryption of Data and Software

IT environments require collaboration across the company. The transit of the data is everywhere, so the best practice is encryption of the data in transit and in rest. Cloud helps to archive this at the file level when files leave and reach it. This means that only limited users can decrypt the files. Keep the IP separate support to create privilege access and encryption of that information. The good part is that monitoring, and Audition can be placed to track operation and keep a sanitise environment. Use cryptographic network protocols is also other technic that helps to hence the secure communications.

Control's security mechanisms for health checks.

The construction of security behaves is repeat steps to check if everything is in place. Management tools support the continuous, and alerting checks. Prevent unauthorized access cleaning former employer accounts. Avoid unnecessary data access, storage, and transmission.

Secure Servers

The suggested architecture is hybrid deployment requires as much as the servers in the cloud as on-premises services protection by firewalls rules and file encryption. Some techniques used to secure the cloud can be used to secure the server. There is other option that is move IP to the cloud the key to keep this secure is storage encryption with services like AWS S3.

3.2 Data Sovereignty

It is data collected which are subject to laws and governance structures within the nation. This is a big concern for DR Alarms due to Australia have strong restrictions for manipulating data. This means that data must keep in datacentres that are physically located in Australia (data residency) and only accessible for Australian people, governments, and industry(Amazon Web Services, 2021c).

Data in Australia are subject and protected by Australian Privacy Principles (APPs) which are 13(Commissioner, 2014). Therefore, the company must follow this principles and also act with the recently Code of Practice, Securing the Internet of Things for Consumers to archive this(Affairs, 2020).

The cloud provider plays an important role in data sovereignty. The cloud provider in this case has to located the data in Australia according to law and regulation(Amazon Web Services, 2020d). AWS implements and maintains technical and organizational security measures applicable to AWS cloud infrastructure services under globally recognized security assurance frameworks and certifications including IRAP, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SOC 1, 2, and 3. These comprehensive AWS technical and organizational measures are consistent with the goals of the APPs to protect personal data. It here where AWS Shared Responsibility Model (Amazon Web Services, 2021n). Have to be clear by the Company and apply the necessary measures to maintain control over their content and are responsible for implementing additional security measures based on their specific needs, including content classification, encryption, access management and security credentials(Amazon Web Services, 2020d).

The following steps that that are recommend archive data sovereignty for the IoT data and IP are:

3.2.1 Categorize what is the data and evaluate where is storage and separate processes

The reasons to do this is warranty the limitations to data needs to found controls and warranty that IoT Data and IP is treated according to data sovereignty in pro of integrity and confidentiality. The

- **Controls**
    - Risk assessment for each category
    - Risk treatment
    - Risk Control
    - Apply polices for management.
    - Constant evaluation of data that is needed to provide a quality service.
    - Document changes

Follow the Australian Privacy Principles (APPs) for collection of data.

These principles are essential to protect Dr alarms customers Data to be manipulated and processed according to the policies.

- **Controls**
    - Plan to achieve every practice.
    - Document
    - Monitoring
    - Auditing

3.2.2 Build the IoT device and keep the IP data according to Code of Practice, Securing the Internet of Things

Follow every practice make sure a security treatment of data secures the data of the customer in pro to archive the data sovereignty.

- **Controls**
    - Plan to achieve every practice.
    - Document internal control
    - Document changes
    - Monitoring
    - Auditing

Demand transparency to the cloud

It is part of the agreement the transparency of cloud compliance.

- **Controls**
    - SLAs need a constant monitoring in pro keep the company safe against laws and regulations this is archivable by the controls implemented to management the cloud.
    - Check changes

Keep an eye over the new laws and ease others.

The laws and regulation change every time which sometimes become in more strong affecting everything even cost or ease some in beneficial of the company.

- **Controls**
    - Revising constantly the local laws and regulation
    - Plan if occur changes.
    - Revising the provides SLA.
    - Training to developer in data sovereignty

The cloud provider and the company have to meet the compliance such as laws and regulation of data sovereignty. The provider must be transparent that they meet the requirements by reporting and monitoring as well as the company also meet them in the same way. Risks of compliance can face severe regulatory penalties and reputation for the company.

4. Proposed BCP for Cloud services

Move to the cloud on many occasions is the best option to include in the BCP for its capability to respond quickly under adverse circumstances. Data should be high available in any case of disaster or incident. Thus, some issues and some advice are giving to be evaluated to be included in the BCP. They are focused to provide application resilience, and backup and disaster recovery capabilities supported by the cloud.

4.1 Resilience

Resilience is more than during operation scale up and down resources while the traffic is having the peak higher. So, Resilience is more like carry the operation while a catastrophe scenario is occurring. The promise that the cloud solves the problem of scalability and flexibility is true while the costumer built enough knowledge to build resilience in its environment. Operation can be managed over the storage, where if an application going down the storage is still feeding the second zone. Thus, any interruption incident should be addressed using multiple data available zones to separate functions and isolate the workflow to be handled (Conferences, 2019). Data replication is an important feature that is well manageable by load balancer to efficiency respond to requests. therefore, Resilience is showed trough different layers, presentation, application, and storage.

4.1.1 Resilience Risks

Operation and data traffic patters

Move to the cloud have advantage for situations that are predictable and unpredictable. Therefore, in a catastrophe the operation and the data traffic patterns change which affect the network in the cloud. Carry a plan to operate in an extreme situation should give in advance in resiliency.

Handle the workflow.

The inexperience to handle the workloads is an important aspect that IP professionals in DR alarms should to learn. Study different scenarios and patterns provide a better understanding of handle it.

Test environment

Have a test environment can cost, but also can avoid waste of money. It supports the operation in advance to any scenario that it is pretending to be use.

Time out failure

This occur when a user make request to the data base and it is nor respond. The run time continue making the request until get failure error.

King data

Move to the cloud is operate in a new cloud environment that had evolved. The data used on-premises was structured different to the actual days. So, match the data to talk with application in the same actual language can avoid error. This means that part of resilience is evolved to solve the problems first before incidents occur.

Scale and load balancers are logic.

Network in the cloud is logic which means that logic can failure. Learn about the patterns designs to improve the architecture is crucial. The common pattern was applied to the DR alarms follow the scaling in a secondary zone if one fail.

4.2 Backup and disaster recovery

Backup and disaster recovery strategy is critical by Dr Alarms. Sensitive data is critical by the company. Therefore, disaster recovery planning around the issues above can hence the results(Amazon Web Services, 2021j). DR strategy should be able to support compliance of SLAs with the clod provider and service level targets of company to their customers(Amazon Web Services, 2018). It also should be able to evaluate the impact and how to resolve business disruption quick and effective. Furthermore, it should contemplate a test environment to carry pre-activities in a safe place before production environment. Activities such as Incidence respond also must consider to be prepared in case a DR need it.

4.2.1 Backup and disaster recovery risks

Handle the complexity of the cloud

The cloud can result complex in design and have many configurations that can not easy to manage quickly if something happened. But having an architecture replica of it can handle management activities such as patching, vulnerabilities test, network changes and others before being applied. It is better to have a problem to resolve than an incident in the entire architecture. It can have benefices in cost, time-consuming and availability. This is a fast and secure failover process.

Recovery from a disaster

Create the plan to back from a disaster is not easy. It must orchestrate in the way to cause the minimal business disruption. Automated disaster recovery are tools to support this task quickly. Therefore, the design should go pro to provide a quick respond.

Backup Management

When occur an incident requires control as soon as possible. System with Automatic control can support a quick respond and create the alerts and notifications. This can be achievable through an environment that allows it. Thus, the management console must be easily reachable to respond.

Accidental detection

Data loss can occur by accidental deletion, system crash or software corruption. Humans can commit mistakes but applying the correct controls and training this can be avoid.

Access to backups

To respond to DR requires access to backups, but what if there is not internet connection? the location where is store the backups is important and also the connection to internet if they will be store in the cloud. According to the case, the architecture was design to store on-premises.

Bandwidth issues

Chucks of data can be heavy, so, download backups requires the right amount of bandwidth to support the recovery.

Recovery time

Disaster recovery can stress the local systems and take time to reach a system operating again. Make a plan around the most important data for minimal operation could safe time.

5. References

Affairs, D. o. H. (2020). *Code of Practice Securing the Internet of Things for Consumers*. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Amazon Web Services, I. o. i. a. (2016). Introduction to AWS Security Processes.

Amazon Web Services, I. o. i. a. (2018). Using AWS in the Context of Common Privacy & Data Protection Considerations.

Amazon Web Services, I. o. i. a. (2019a). *Securing the Microsoft Platform on Amazon Web*. https://d1.awsstatic.com/whitepapers/aws-microsoft-platform-security.pdf

Amazon Web Services, I. o. i. a. (2019b). *Web Application Hosting in the AWS Cloud: Best Practices*. https://docs.aws.amazon.com/whitepapers/latest/web-application-hosting-best-practices/web-application-hosting-best-practices.pdf

Amazon Web Services, I. o. i. a. (2020a). *Guidelines for Implementing AWS WAF*. https://d1.awsstatic.com/whitepapers/guidelines-implementing-aws-waf.pdf

Amazon Web Services, I. o. i. a. (2020b). *Hybrid Cloud with AWS*. https://d1.awsstatic.com/whitepapers/hybrid-cloud-with-aws.pdf?did=wp_card&trk=wp_card

Amazon Web Services, I. o. i. a. (2020c). *Microsoft SharePoint Server 2019 on the AWS Cloud*. https://fwd.aws/B43QY

Amazon Web Services, I. o. i. a. (2020d). *Using AWS in the Context of Australian Privacy Considerations*. https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf

Amazon Web Services, I. o. i. a. (2021a). *Amazon ElastiCache*. https://aws.amazon.com/elasticache/redis/

Amazon Web Services, I. o. i. a. (2021b). *Amazon Route 53*. https://aws.amazon.com/route53/

Amazon Web Services, I. o. i. a. (2021c). *Australia Data Privacy*. https://aws.amazon.com/compliance/australia-data-privacy/

Amazon Web Services, I. o. i. a. (2021d). *AWS CloudFormation*. https://aws.amazon.com/cloudformation/

Amazon Web Services, I. o. i. a. (2021e). *AWS Cloudwatch*. https://aws.amazon.com/cloudwatch/

Amazon Web Services, I. o. i. a. (2021f). *AWS Identity and Access Management*. https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Amazon Web Services, I. o. i. a. (2021g). *AWS Key Management Service (KMS)*. https://aws.amazon.com/kms/

Amazon Web Services, I. o. i. a. (2021h). *AWS Secrets Manager*. https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Amazon Web Services, I. o. i. a. (2021i). *AWS WellArchitected Framework*. https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf

Amazon Web Services, I. o. i. a. (2021j). *Disaster Recovery of Workloads on AWS: Recovery in the Cloud*. https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html

Amazon Web Services, I. o. i. a. (2021k). *Elastic Load Balancing*. https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html

Amazon Web Services, I. o. i. a. (2021l). *Internet gateways*. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Amazon Web Services, I. o. i. a. (2021m). *NAT gateways*. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Amazon Web Services, I. o. i. a. (2021n). *Shared Responsibility Model*. https://aws.amazon.com/compliance/shared-responsibility-model/

Amazon Web Services, I. o. i. a. (2021o). *Ten security golden rules for IoT solutions*. https://aws.amazon.com/blogs/iot/ten-security-golden-rules-for-iot-solutions/

Cidon, A. (2015). Protecting Intellectual Property in the Cloud. *WIPO Magazine*.

Commission, A. a. t. a. I. (2021). *Australian Intellectual Property laws*. https://www.austrade.gov.au/international/invest/guide-to-investing/running-a-business/understanding-australian-business-regulation/australian-intellectual-property-laws

Commissioner, O. o. t. A. I. (2014). *Australian Privacy Principles*. https://www.oaic.gov.au/privacy/australian-privacy-principles/

Conferences, N. (2019). *Patterns for Resilient Architecture - Adrian Hornsby*. https://aws.amazon.com/blogs/architecture/architecture-patterns-for-red-hat-openshift-on-aws/

Erl, T., Mahmood, Z., & Puttini, R. (2013). *Cloud computing : concepts, technology, & architecture* (1st edition ed.). Prentice Hall.

Justyna Kucharczak, & Inc, S. U. (2020). *The Egregious 11: Examining the Top Cloud Computing Threats*. https://www.securit.biz/securit-news/the-egregious-11-examining-the-top-cloud-computing-threats

Lord, N. (2020). *How to secure intellectual property from loss or compromise*. https://digitalguardian.com/blog/how-to-secure-intellectual-property