**MIS607 – CYBERSECURITY**

**ASSESSMENT TITLE – MITIGATION PLAN FOR THREAT REPORT**

**STUDENT NAME:** MOHAMMED ZHOEB

**STUDENT NUMBER** – 00287693T

**LECTURER:** 1. DR.SHAHRZAD SAREMI

2. DR.AZAM SHIRRAFIARDEKANI

TRIMESTER 3(2020)

**TABLE OF CONTENTS**

Introduction……………………………………………….3

DFD…………………………………………………………….3

THREAT MODELLING………………………………….5

RISK ANALYSIS…………………………………………..8

MITIGATION PLAN…………………………………….12

BUSINESS IMPROVEMENT MODEL……………16

SIGNIFICANCE…………………………………………..18

CONCLUSION…………………………………………..18

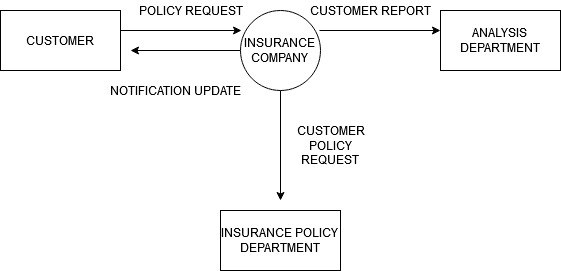
RECOMMENDATIONS………………………………19

REFERENCES…………………………………………….20

**Introduction:** The below report illustrates about the mitigation plan which is been defined as an increment in opportunities by developing different options by customized plans to reduce threats or vulnerabilities (Ahmed, 2017). The various DFD depicts the operational functionality of the B&C insurance company along with the threats which is been modelled using stride methodology. The risk analysis has been performed to find the risk appetite and various mitigation plans has been generalized. The report also conceptualizes the business improvement model for effective business cyber model along with its significance.

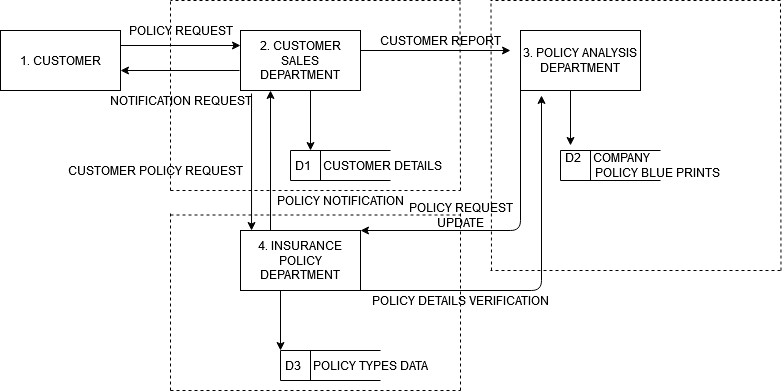
**Note:** The DFD and threat modelling was done again based on the comment on assessment 2 by Shazi.

**Context diagram: (DFD)**

****

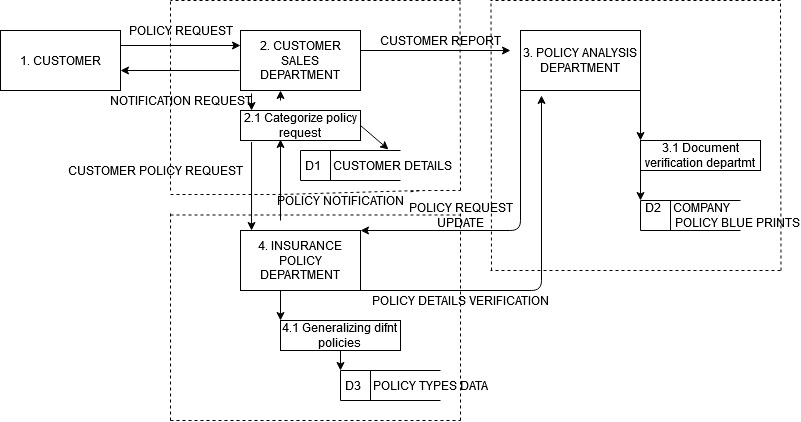
The above context diagram represents customer, insurance policy department, analysis department as external entity and insurance company as main process within the system. The flow of data is been represented by the arrow.

**Level – 0**

****

The level- 0 DFD represents the data flow of B&C Insurance company with all the external entities and D1, D2, D3 represents the data stores of the company. 2. Customer sales department is the further explanation of the insurance company respectively. The policy request is been sent to the sales department where the report is sent to the analysis department and policy request is sent to the insurance policy department. Request update is send to the insurance policy department. Each process has its own trust boundaries which are vulnerable to the attack.

**Level – 1:**

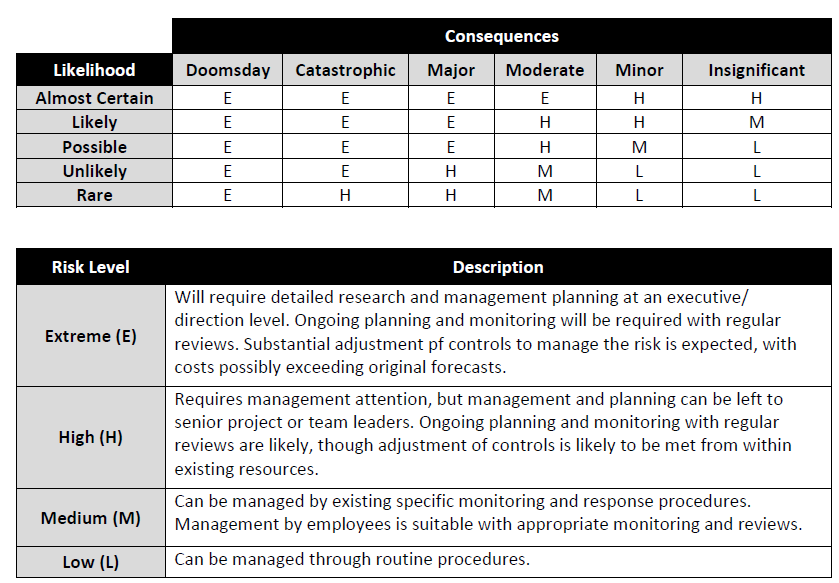
****

The level -1 is further expansion of level -0 diagram which have sub process like 2.1 categorize policy request which adds certain department within the customer sales department process. 4.1 generating different policies and 3.1 document verification department acts in the same way to respective process.

**Threat modelling:**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Attacker Intention** | **Threat to B&C Insurance** |
| Spoofing of machine | Miss connecting the IP address of the servers (ARP spoofing)  Sending the packets to main server in disguise of genuine user (IP spoofing) | The attacker might generate an IP address as one of the genuine server and might gather information regarding the customer details between one server of the company to the other server.  The attacker might send the request to gain the login details of the customer to get into the account of it. |
| Spoofing name | Creating fake identity emails. | The attacker might send the email in a disguise of the insurance company employee to gain information. For example sending the email as a regional manager of the insurance company requesting the card details for package upgrade. |
| Tampering the code  Tampering of API gateway | Code tampering can be done in the DB  The security layer of company can be disintegrated. | The attacker might tamper the code of the B&C main site like policy detail sets making unavailable to view the web pages.  The attacker might breach the security layer which might avoid the key tokens for login into the company site. |
| Repudiation | Making the entry of data into logs | The attacker might add data into the logs of the system after accessing into the insurance company to avoid distraction from the company employee as most of the hackers do not leave their details. |
| Information disclosure by creating SQL bugs | Gaining the entry by creating fake queries. | The attacker might gain entry within the B&C insurance company database to look over the details of company customers like date of application, policy cover etc. |
| Information disclosure by analysing the flow of traffic | Flow of data in more number can be viewed by the attacker | As the B&C is a multi-national company the attacker might watch data flow to find out which country has more users. |
| Denial of service by creating fake temp files  Denial of service by creating multiple accounts | More temp files might slow down the system  Multiple accounts are been created by the attacker | The attacker might create more temp files within the B&C server making the server slow down.  The attacker might create multiple accounts in the insurance company which might slow down the server or fail the server as each of the account creates a data in server. |
| Elevation of privilege by company employees | Company employee might experience more access to the information than they are assigned to. | The attacker might possess threat to B&C like approving policies to the customer that they are not eligible for it. |

**Risk Analysis:**

****

**RISK ANALYSIS:**

|  |  |
| --- | --- |
| **Thread description**: Miss connecting IP address (ARP spoofing) | |
| **Risk level:** Extreme | **Consequence:** Major |
| As it is a multinational company having different sub servers might exposed to this threat. | **Rating:** Likely |
|  |
| **Improvement techniques:** Using secure ARP technique might solve issue. |

|  |  |
| --- | --- |
| **Thread description**: Spoofing name | |
| **Risk level:** Extreme | **Consequence:** catastrophic |
| As it is operated in different regions can face this type of threat. | **Rating:** certain |
|  |
| **Improvement techniques:** This threat can mitigated using patch based kernel using antidote approach. |

|  |  |
| --- | --- |
| **Thread description**: Tampering the code | |
| **Risk level:** Extreme | **Consequence:** major |
| As the attacker had already got into the system might have extreme risk level.  . | **Rating:** possible |
|  |
| **Improvement techniques:** Routing methods can be used to improve the threat in B&C insurance |

|  |  |
| --- | --- |
| **Thread description**: **Tampering API gateway** | |
| **Risk level:** high | **Consequence:** moderate |
| As the security had already been breached for the B&C it might breached again. | **Rating:** possible |
|  |
| **Improvement techniques:** This threat can be mitigated by knowing the API inventory, regulations and tracking vulnerabilities. |

|  |  |
| --- | --- |
| **Thread description**: Data entry into logs | |
| **Risk level:** extreme | **Consequence:** major |
| Due to vast number of customers it might be misleading the employee by such actions by attacker. | **Rating:** possible |
|  |
| **Improvement techniques:** addition of AAA server within the B&C insurance company. |

|  |  |
| --- | --- |
| **Thread description**: **SQL injections** | |
| **Risk level:** extreme | **Consequence:** major |
| It is one of the most common threat types in public companies. | **Rating:** likely |
|  |
| **Improvement techniques:** creating a customized page to showcase the less information of DB |

|  |  |
| --- | --- |
| **Thread description**: **Flow analysis** | |
| **Risk level:** high | **Consequence:** moderate |
| Due various branches throughout world might be exposed to this type. | **Rating:** possible |
|  |
| **Improvement techniques:** using the OPNET and Netsim tools in NIDS system within the B&C can improve. |

|  |  |
| --- | --- |
| **Thread description**: Dos attack by temp and multiple accounts | |
| **Risk level:** extreme | **Consequence:** major |
| Reason might be due to competitors to fall out the company behind in the market. | **Rating:** likely |
|  |
| **Improvement techniques:** This technique can be mitigated by upstream filtering method and B&C should outsource the security task to the third party. |

|  |  |
| --- | --- |
| **Thread description**: Elevation of access | |
| **Risk level:** extreme | **Consequence:** major |
| As it is type of financial company operating good money might be exposed to this threat type by insider of company. | **Rating: almost** certain |
|  |
| **Improvement techniques:** B&C should limit the access control, secure the DB and update their systems. |

**Mitigation plan:**

**Spoofing of a machine:**

Mitigation techniques which are based on cryptography consist of two methods like secure ARP (S-ARP) and patches based on Kernel.

**S-ARP:** In this method of ARP spoofing mitigation of the threat can be done by providing the main certificates for authentication within the network for each and every ARP reply. The authoritative key distributor acts as a main server granting the keys to the various hosts making the use of secure DHCP rather than normal DHCP.

**B&C insurance company:** Addition of key distributive server of the company might provide the authentication tokens to every user like customers whenever they try to login from secure DHCP than usual DHCP.

**Patches based on Kernel**: The most used approach called Antidote is been applied in which host when receives ARP reply from the MAC address which is not been similar to the last reply make sure that the last reply MAC address in the cache is alive and banning the threat MAC address and rejecting the network (Tripathi & Mehtre, n.d.).

**B&C insurance company:** Every login attempt made by the B&C insurance user MAC address should be stored in the temp or cache and had to be rectified banning the unknown user login within the network.

**IP Spoofing:**

**Routing methods:** Packets which are routed to its organization helps in the detection of IP spoofed packet entering within the network. Making the traffic flow from internal IP to NAT table and then to the IP present externally to reach the destination (Shyamala & Visalakshi, 2015).

**B&C insurance** company should deploy this method in security layer of application allowing only egress filtering spoofed packets which are not allowed within the network and ingress filtering disallows the packets from the network.

**Identity Spoofing:**

**Multi-factor Authentication:** Multi factor authentication is been used to overcome the attacker by providing passwords, pins, providing token based PIN like one time password, retina scan, fingerprint scan etc. As most of the attackers have multiple attacking skills to overcome the system which can be minimized by using multi factor authentication method (Michael Stewart, 2018).

**B&C** can provide an extra step in login application of providing a one-time password and a six digit pin to the mobile phone to have secure login.

**Tampering:**

**Tampering of code within DB:**

**Block chain solution:** It is vast decentralized data base mostly shared within the public or private network. Block chain database provide the transactions to occur within the users verifying the user and preventing the transaction that is meant to be unauthorized. Data present within the block chain is mostly impossible to alter or change enhancing more security to the data of the business (Iqbal, 2019).

**B&C** should store all the customer details as a verified user within the block chain data base which is hard to be altered, this provides an authorized transaction like payment of the policies to the company by the genuine user rather than the third party.

**Tampering the network layer: (API gateway)**

As the breach of the customer data in B&C might occur by altering the API gateway and tampering the security network. To maintain the API more secure three steps has to be followed:

**Knowing the inventory of API:** B&C insurance has to maintain a clear API inventory to know the unprotected API in the system by documenting the APIs that has been inventoried. According to the researchers it was found that most of the organizations have a gap of about 40% between the API that has been inventoried and which has actually deployed.

**Auditing legal regulations:** After the inventory of the API all the parameter has to be mapped more effectively and should be audited legally. Delivery pipeline should be incorporated with the continuous testing process and the API teams has to consider the security and legal protocols whenever there is a new update in the system.

**Tracking the vulnerabilities:** There exist more security gaps within the API which include broken keys, tokens which are unexpired might be hijacked etc which might possess threat to the system. To overcome this issue OWASP have developed a resource of top vulnerabilities which are been rallied behind by most of the companies as most of the organization in the world should adopt to these OWASP issues (Doerrfeld, 2020).

**Repudiation:**

**Insider threat:** (creating data entry in logs to distract the users)

It is also a kind of insider threat who gains unauthorized access within the system by the employee of the organization, who creates data in the logs to distract the authorized users. This threat can be mitigated by using **centralized authentication for user.**

**Centralized authentication for user:** All the device access has to be given only to the authorized personnel having an separate secure account and password. All the accounts that are been assigned to the authorized personal has to be managed by the central server (AAA server (Authentication, Authorization and Accounting server) enforcing all the security policies like assigning limit on unsuccessful attempts, role based control, strength of the password rules etc (Tsegay Tesfay & Hubaux, 2014).

**B&C insurance** can use AAA server who provide access control roles to its employee and also to its customers. As the customer edit their personal details on their own which are not been visible to the employee and done directly within the server itself and can block the individual when their role within the insurance is not much longer needed or suspected as malicious attempt on the analysis of the logs.

**Information Disclosure: (SQL injection with the DB)**

SQL injection threat can be mitigated by using the approach of input validation method.

**Input validation method:**

It is the method which process the unauthorized network directing to the error page that is been customized showing less information error to the user making user having less DB information preventing the SQL injection threat based on inspecting its length, format, range and type of its unauthorized user (Teckchandani, 2018).

**B&C** should design a customized error page to the front end users distracting from the actual database information. The actual error report has to be sent to the authorized personal involved in solving the issue to fix the error who has been granted permission from the AAA server.

**Flow of data traffic intrusion:** In this method the hacker analyses the flow of data traffic among the network. This threat can be mitigated by using **Network intrusion system of detection.**

**Network intrusion system of detection:** In this method detection systems are been placed within the points of the network to monitor the flow of traffic in and out of the system analysing the traffic on the entire subnet. Any un usual activities which has been detected is been alerted by the administration (Niyaz & Sun, 2016).

As the **B&C** is been operated worldwide, the flow of data takes place from user to the sub server of each respective country and then to the main centralized server. The NIDS system should be placed at each point using the common tools like OPNET and Netsim can help in detecting the flow of traffic coming from external network to avoid any threat to the system.

**Denial of service: (Generating multiple temp files and accounts)**

**Upstream filtering method:** In this method of mitigation it routes the flow of data through various network system which identifies the traffic which is found to be malicious. Some of the external providers offers protection by analysing incoming packets of IP from the attacker or the bot allowing the only legitimate traffic flow of data. Most of the API gateway does function in the same way but also filter the flow based on endpoints that are requested, HTTP verbs or combination of both (Unni, 2016).

**B&C** should outsource the security task to the external providers like Amazon and cloudfront who might make them responsible for the various DOS attacks making company to focus more on service buildings.

**Elevation of Services: (Modifying the code)**

Most of the elevation of service causes the user to gain access to the controls that they are not authorized to, making the system default or corrupt either by SQL injections of modifying the code to make server imbalance.

This threat can be mitigated by **B&C** by following these steps:

**Allowing users with minimum access:** User base has to be reviewed with minimum accounts and user controls with predefined role and they have to be set with minimum access. Removing the user when their role is not much needed has to be done.

**Securing database and user inputs:** Data base should be secured by using strong authentication protocol and encrypting most of the data whenever it is at rest. All the user inputs should be sanitised to prevent SQL and other code injections.

**Securing the system and application by patching and update:**

Repetitive scan has to be done to find out the vulnerabilities in the application and security patch has to be applied, as large scale production system cannot be updated manually they has to be applied additional layer of security on it (Cassetto, 2020).

**Business improvement model:**

**Knowing and understanding the risk:**

It is the first step involved in improving the risk management practices of the B&C Company which can be done by categorizing and assessing the data and assets of the company to know the scope. As the scope has been identified it analyse the threat against the data and assets of the company to control the risk.

**Mapping out the management plan:**

Creating a divisive strategy will help the organization to prepare and respond to threats. As the threats are unpredictable they can be mitigated. Procedure development, policy and process should be a part of the plan.

**Employee training:**

The importance of the cyber security plan has to be educated well to all the employees and making procedure, process and policy as a part of regular training sessions. Every employee of the company should support the cyber security risk management plan will help in mitigating the risk ("How to Improve Your Company’s Cyber security Risk Management", 2020).

**Involvement of the executive level:**

Top level executives of the company should also be involved in the security solutions as well not just the business strategies as most of the technologists have issues in explaining the complex security relation solutions to the top level executives.

**Value chain risk assessment:**

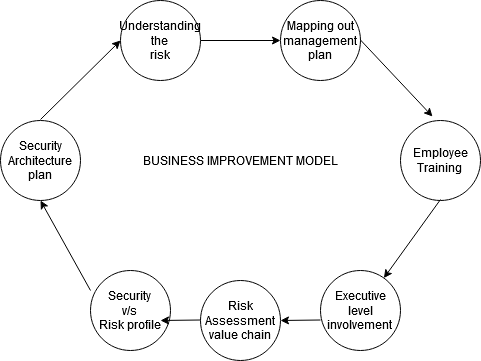
Data has to be identified where it is accessed by different stakeholders of the company to find out which is more sensitive arising more challenges. Data that is found to be more sensitive should be made to put more efforts in securing the highest risk data. Dividing it into sub components like differentiating credit card number and CVV number in different database, can help in mitigating the risk.

**Balancing the security, impact and expenses v/s risk profile:**

Most of the companies add basic techniques of security at the initial layer of security to vast amount of data. Data that represents high risk should be protected well in comparison to normal operational business data.

**Security architecture development:**

For most of the large organizations layered approach found to be efficient. The sensitive data has to be secured by using multiple approaches making the intruder ineffective to break the security border. B&C should also develop security architecture to improve its business model. (Dillard, n.d.).



**Significance:**

A better cyber security model helps in making more strategic decisions.

It helps to gain more profits as the brand is well protected and trusted by the customers

Organization insights can be bought under the notice of board of directors.

It reduces the liabilities of the business

It helps to meet the company with more compliance standards ("How to Improve Your Company’s Cybersecurity Risk Management", 2020).]

**Conclusion:** The above reports have discussed the DFD of the B&C insurance company along with various threats. It represents the severity of the risk using the risk analysis method to script the effective mitigation plan to mitigate the threats that the company might face ahead. To have an effective business structure improvement model has also been suggested within the report along with its significance.

**Recommendations:**

Wheeler, E. (2011). Security Risk Management. Retrieved from <https://www.sciencedirect.com/book/9781597496155/security-risk-management>

F. Broder, J. (2012). Mitigation and Preparedness. Retrieved from http://Mitigation Plan for Threat Report

Parker, D., & Mobey, A. (2004). Action Research to Explore Perceptions of Risk in Project Management. International Journal of Productivity and Performance Management 53(1), 18–32.

Gomes, J., & Iivari, M. (2018). Cyber Security Business Models in 5G. Retrieved from https://www.researchgate.net/publication/322466981\_Cyber\_Security\_Business\_Models\_in\_5G

**References:**

Ahmed, R. (2017). Chapter 5 Risk Mitigation Strategies in Innovative Projects. Retrieved from https://www.researchgate.net/publication/319400764\_Risk\_Mitigation\_Strategies\_in\_Innovative\_Projects

Tripathi, N., & Mehtre, B. Analysis of various ARP Poisoning mitigation techniques : A comparison.

Shyamala, K., & Visalakshi, S. (2015). Mitigating IP Spoofing to Enhance Security in Multi-Agent based e-Learning Environment. doi: 10.17485/ijst/2015/v8i17/63910

Michael Stewart, J. (2018). The Three Types of Multi-Factor Authentication(MFA). Retrieved from <https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/>

Iqbal, M. (2019). Comparison of Blockchain-based Solutions to Mitigate Data Tampering Security Risk.

Doerrfeld, B. (2020). Strengthen API Security With These Tips and Patterns.

Tsegay Tesfay, T., & Hubaux, J. (2014). Cyber-secure Communication Architecture for Active Power Distribution Networks.

Teckchandani, T. (2018). SQL injection attacks and mitigations Computer application security capstone project. Retrieved from <https://www.grin.com/document/461503>

Niyaz, Q., & Sun, W. (2016). A Deep Learning Approach for Network Intrusion Detection System.

Unni, A. (2016). Denial of service attacks: Methods used to prevent them. Retrieved from <https://www.stickman.com.au/denial-of-service-attacks-methods-used-to-prevent-them/>

Cassetto, O. (2020). Privilege Escalation Detection: The Key to Preventing Advanced Attacks. Retrieved from <https://www.exabeam.com/ueba/privilege-escalation/>

("How to Improve Your Company’s Cybersecurity Risk Management", 2020). (2020).

Dillard, J. Six Steps to a Better Cybersecurity Model. Retrieved from https://www.bigskyassociates.com/blog/bid/332473/Six-Steps-to-a-Better-Cybersecurity-Model