

**IT3010**

**Information Assurance and Security**

**3rd Year, 2nd Semester**

**Risk Management Assignment**

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

27.09.2020

**Table of content**

[1. Introduction 3](#_Toc18370033)

[2. Risk Scenarios 4](#_Toc18370034)

[3. Allegro – Worksheet 5](#_Toc18370035)

1. [Risk Scenario 1 5](#_Toc18370036)
2. [Risk Scenario 2 7](#_Toc18370037)
3. [Risk Scenario 3 9](#_Toc18370038)
4. [Risk Scenario 4 11](#_Toc18370039)
5. [Risk Scenario 5 13](#_Toc18370040)

[4. Appendix 15](#_Toc18370041)

1. [Justification of probability and Severity values of Risk Scenario 1 15](#_Toc18370042)
2. [Justification of probability and Severity values of Risk Scenario 2 16](#_Toc18370043)
3. [Justification of probability and Severity values of Risk Scenario 3 18](#_Toc18370044)
4. [Justification of probability and Severity values of Risk Scenario 4 19](#_Toc18370045)
5. [Justification of probability and Severity values of Risk Scenario 5 20](#_Toc18370046)

[5. References 22](#_Toc18370047)

1. Introduction

PolyTech plastics (Pvt) Limited, is a Sri Lankan based company. The mission statement of this company is to supply the local and international market with high quality plastic items, such as chairs, tables, utensils, brooms etc.

When the company first started most of the processes were handled manually, by maintaining records and ledge PolyTech plastics (Pvt) Limited, is a Sri Lankan based company. The mission statement of this company is to supply the local and international market with high quality plastic items, such as chairs, tables, utensils, brooms etc.

When the company first started most of the processes were handled manually, by maintaining records and ledgers, but the manual system soon became obsolete as the business grew, maintaining a manual system incurred losses to time and resources and since the number of transactions increased exponentially it became very tedious and the system was error prone

To overcome the above the problem the company started using a computerized web-based system called PolyTechSys which was custom made for the purposes of the company. Using this system all employees of the company from sales reps to top level managers were able to perform effectively and efficiently thus boosting the productivity of the company. The system was built including several user layers so that sensitive information and certain other information does not end up in the wrong hands thereby assuring secrecy and security. Usually top level managers have access to most of the sensitive information stored in the system such as sales data,customer data, salary info etc. In addition to the above users product distributors also have access to the system. These distributors enter sales data in to the system and their performance is monitored by top level managers.

The purpose of this document is to recognize the critical assets in the company and identifying the potential threats and risk scenarios which could impair the day to day functioning of the company. Once the risk scenarios are identified we can compile them in Allegro worksheets and then predict the probability level for all the risk scenarios based on a good justification and also propose risk mitigation techniques for each risk scenarios, but the manual system soon became obsolete as the business grew, maintaining a manual system incurred losses to time and resources and since the number of transactions increased exponentially it became very tedious and the system was error prone

To overcome the above the problem the company started using a computerized web-based system called PolyTechSys which was custom made for the purposes of the company. Using this system all employees of the company from sales reps to top level managers were able to perform effectively and efficiently thus boosting the productivity of the company. The system was built including several user layers so that sensitive information and certain other information does not end up in the wrong hands thereby assuring secrecy and security. Usually top-level managers have access to most of the sensitive information stored in the system such as sales data, customer data, salary info etc. In addition to the above user’s product distributors also have access to the system. These distributors enter sales data in to the system and their performance is monitored by top level managers.

The purpose of this document is to recognize the critical assets in the company and identifying the potential threats and risk scenarios which could impair the day to day functioning of the company. Once the risk scenarios are identified we can compile them in Allegro worksheets and then predict the probability level for all the risk scenarios based on a good justification and propose risk mitigation techniques for each risk scenario

1. Risk Scenarios

**Risk Scenario 1 (Data Breach)**

The top-level users of the system have access to sensitive information such as customer emails, and other private information which are stored in the system. This set of information can be exploited via selling them to outsiders for profit

**Risk Scenario 2 (Unauthorized data modification by SQL Injection)**

The attacker finds a way to access the database of the company and modify the legitimate

data, this attack is carried out via modifying SQL queries that interact with the database of the company. Usually the attacker needs to find a page in which he can interact with the database of the system(for example login page) then the attacker modifies the underlying query statements to gain unauthorized access to the database schema, using the schema the attacker can now modify the data stored in the database

**Risk Scenario 3 (DDOS attack using SYN Flood)**

Attacker tries to overload the main server of the company by sending distributed connection requests (often by sending multiple SYN packets to the server) thereby preventing the legitimate users from using the main server

**Risk Scenario 4 (Take Administrative access to the system by Baiting Attack)**

Here the attacker exploits the human curiosity to perform this attack. The attacker leaves a physical storage device such as a USB storage device in the company premises, Employees find this device and connect it to their office computer to know it’s contents. As soon as the device is connected, the rootkit program in the device will get installed in the system and it provides a way through which the attacker can gather sensitive information.

**Risk Scenario 5 (Targeted Ransomware)**

The attacker creates spam emails that look like emails from legitimate sites and send them to multiple employees of the company. Usually these emails have links in them or downloadable content in the attachments, when employees interact with such emails, usually a ransom-ware is set up by the attacker to slowly start encrypting all the data in the hard disk of the target device and sometimes if the target device is connected to the company network, the ransom-ware spreads through the network to the other computers and start encrypting the data, thereby preventing legitimate users from accessing necessary data. After encryption is successful a message will be displayed to the user which contains the details of payment to remove the ransom-war

1. Allegro – Worksheet
   1. Risk Scenario 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Sensitive and valuabledetails of the customer | | | | | |
| Area of Concern | *Data Breach* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Insider (Staff Member who has access) | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The internal staff member who has administrative access to the sensitive data, sell that details to the outsiders who are looking for that details for a profit | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Intentional | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Ensuring that critical data of the customers should be accessible by authorized persons and sensitive data of customers, in the outsider can cause for financial issues. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **(75%)** | * **Medium**   **(50%)** | | * **Low**   **(25%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| When the sensitive data of the customer are exposed to a third party, the reputation of the company will be diminished as a result customers will be disappointed and they’ll be afraid to trade with the company. Because of that the financial stability of the company will be affected | | | | Reputation & Customer  Confidence | | 9 | 6.75 |
| Financial | | 7 | 5.25 |
| Since the customers are disappointment, customers will not initiate trades with the company. Because of that the product sales will be reduce.Decrease in sales decrease the production | | | | Productivity | | 7 | 5.25 |
| Safety & Health | | 0 | 0 |
| Customers might take legal actions against the company which can cost a large amount of company resources to handle. (Ex : Hiring Lawyer) | | | | Fines & Legal Penalties | | 6 | 4.5 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **21.75** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Legal Actions | After finding out the culprit, the company has to take legal actions against that employee, recover compensations and dismiss the culprit | | | |
| Conducting awareness programs | Conduct a proper awareness program for new and existing new employees of the company and keep the employees updated about the threats that may affect to the company reputation | | | |
| Hiring right person to the job | When hiring a person for the one of the main roles of the company, there should be a procedure to make sure he/she will be the right person to this job by looking into his/her background details, employee history and references. | | | |

* 1. Risk Scenario 2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Customer Database | | | | | |
| Area of Concern | *Unauthorized data modification by SQL Injection* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Outsider(Hacker) | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The attacker finds a way to access the database of the company and modify the legitimate data, this attack is carried out via modifying SQL queries that interact with the database of the company. Usually the attacker needs to find a page in which he can interact with the database of the system(for example login page) then the attacker modifies the underlying query statements to gain unauthorized access to the database schema, using the schema the attacker can now modify the data stored in the database | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Intentional | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Company needs to maintain a Backup of the database. Make sure that the database can only be accessed by the authorized people of the company. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **(75%)** | * **Medium**   **(50%)** | | * **Low**   **(25%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| Customers of the company will be disappointed and dissatisfied with the company because they have no proper backups of the database which contains personal details, critical details as well as the purchase details. In addition of that the reputation of the company will be damaged because the company could could not protect their assets properly.  . | | | | Reputation & Customer  Confidence | | 7 | 5.25 |
| Financial | | 5 | 3.75 |
| Since the customers are disappointment, customers will not initiate trades with the company. Because of that the product sales will be reduce.Decrease in sales decrease the production | | | | Productivity | | 7 | 5.25 |
| Safety & Health | | 0 | 0 |
| Customers might take legal actions against the company which can cost a large amount of company resources to handle. (Ex : Hiring Lawyer) | | | | Fines & Legal Penalties | | 5 | 3.75 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **18** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Update and patch | vulnerabilities in applications and databases that hackers can exploit using SQL injection are regularly discovered, so it's vital to apply security patches and updates regularly. | | | |
| Firewall | Consider a web application firewall (WAF) that can be particularly useful to provide some security protection against a new vulnerability before a patch is available  . | | | |
| Buy better software | Make code writers responsible for checking the code and for fixing security flaws in custom applications before the software is delivered. | | | |

* 1. Risk Scenario 3

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Web Server | | | | | |
| Area of Concern | *DDOS attack using SYN Flood* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Outsider(Hacker) | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The attacker sends a large volume of SYN packets to the targeted web server, often with spoofed IP addresses. The server responds to each one of the connection requests and leaves an open port ready to receive the response. The server waits for the final ACK packet to arrive, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the server is overloaded and unable to function normally. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Intentional | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | The total system will be inaccessible due to the web server failure. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **(75%)** | * **Medium**   **(50%)** | | * **Low**   **(25%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| When a DDOS attack happens to the system, reputation of the brand/ company will be damaged. As well as, because of DDOS attack confidential data will be lost. | | | | Reputation & Customer  Confidence | | 8 | 6 |
| Financial | | 7 | 5.25 |
| This system is also use by the sales representatives of the company for invoicing. When the server gets down by the DDOS attack sales representative will not be able to reach the online platform for invoicing | | | | Productivity | | 5 | 3.75 |
| Safety & Health | | 0 | 0 |
| The productivity of the employees will be decrease. | | | | Fines & Legal Penalties | | 3 | 2.25 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **17.25** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Micro Blocks | administrators can allocate a micro-record (as few as 16 bytes) in the server memory for each incoming SYN request instead of a complete connection object. | | | |
| SYN Cookies | using cryptographic hashing, the server sends its SYN-ACK response with a sequence number that is constructed from the client IP address, port number, and possibly other unique identifying information. When the client responds, this hash is included in the ACK packet. The server verifies the ACK, and only then allocates memory for the connection. | | | |
| RST Cookies | for the first request from a given client, the server intentionally sends an invalid SYN-ACK. This should result in the client generating an RST packet, which tells the server something is wrong. If this is received, the server knows the request is legitimate, logs the client, and accepts subsequent incoming connections from it. | | | |
| Stack Tweaking | administrators can tweak TCP stacks to mitigate the effect of SYN floods. This can either involve reducing the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections. | | | |

* 1. Risk Scenario 4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | All sensitive data in the system | | | | | |
| Area of Concern | *Take administrative access to the system by Baiting Attack* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Outsider | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | Attackers can also focus on exploiting human curiosity via the use of physical media (such as Pen drives). That means the attacker leave a physical device (USB Pen drives) in the company premises. That USBs will contain a rootkit. Curious, many of the employees picked up that USBs and plugged them into their computers. After plugged the rootkit will activated and attacker will get the administrative privileges to the system [4] | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Intentional | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | By having administrative access to the system outsider can do any modification all the data in the system. When sensitive data of the organization, manage by a wrong person can cause for major financial loses. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **(75%)** | * **Medium**   **(50%)** | | * **Low**   **(25%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| When outsider get administrative privileges to the system and he/she will access all the information including both sensitive data of the customers and the company. Because of that company is responsible for investigating on the security threat. | | | | Reputation & Customer  Confidence | | 8 | 6.0 |
| Financial | | 7 | 5.25 |
| Investigating about the attack will take excessive hours of effort. Because of that the productivity of the employees will decrease and company might spend huge amount of money on investigation. | | | | Productivity | | 6 | 4.50 |
| Safety & Health | | 0 | 0 |
| Sometimes customers will take legal actions against the company because of their sensitive details will disclosure to a third party. | | | | Fines & Legal Penalties | | 5 | 3.75 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **19.5** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Conduct awareness sessions | The employees should be given a proper induction on data security when employing them. Even after the initial induction it is important to keep the employees updated about the possible attacks and new risks. | | | |
| Antivirus Software | By installing proper antivirus software to the machine can detect those kinds of malwares and it will control those kinds of attacks that can happen to the company. | | | |

* 1. Risk Scenario 5

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Database of the system and other important files in the computer. | | | | | |
| Area of Concern | *Encrypt the database and other important files in the computer using Targeted Ransomware* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Outsider or Insider | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The attacker will design spam emails to look like it is coming from a legitimate email address and send that emails to the employee’s emails. When receiving that email employees will download and open the email because that email is looks like a legitimate email. When employee download and open the email, then the ransomware will start encrypting all data saved on the employee’s hard disk and even to other computers that is sharing the same network. After the employee’s screen will display the “ransom note” that contain the instructions on how and where you will pay the ransomware attacker in exchange of the necessary decryption passkey. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Intentional | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Both sensitive data of the customers and company and important files, in the wrong hands can cause major financial loses. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **(75%)** | * **Medium**   **(50%)** | | * **Low**   **(25%)** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| When the attacker encrypts both sensitive data of the customers and the company as well as important files, they will be temporary unavailable for the system users. Because of that company will responsible for this issue. As a result of that customers will be disappointed, and the reputation will be damaged. | | | | Reputation & Customer  Confidence | | 7 | 5.25 |
| Financial | | 8 | 6.0 |
| Company might be pay huge amount of money to the ransomware attacker in exchange of the necessary decryption passkey. | | | | Productivity | | 6 | 4.50 |
| Safety & Health | | 0 | 0 |
| When ransomware attack happens to the system/machines, they will not perform accordingly. The ransomware attack can damage of hostage systems, data, and files. Because of that employees will take lot of time to implement backup methods. As a result of that the productivity will be decrease. | | | | Fines & Legal Penalties | | 5 | 3.75 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **19.5** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Conduct awareness sessions | The employees should be given a proper induction on data security when employing them. Even after the initial induction it is important to keep the employees updated about the possible attacks and new risks. | | | |
| Surveillance | Manage internal and external communication channels and other data transformation methods frequently. Restrict inappropriate files sharing with external parties, (ex - control external mail channels) | | | |
| Firewall | Firewall helps to filter out malicious data. Good ones will have a comprehensive set of default rules and make it easy to add new ones whenever necessary. A WAF can be particularly useful to provide some security protection against a new vulnerability before a patch is available. | | | |
| Set Standards | Set internal standards for install software inside the company. Always ask for administrative access to install a software | | | |
| Install proper software | Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place. | | | |

1. Appendix
   1. Justification of probability and Severity values of Risk Scenario 1

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Justification** |
| **Probability** | 75% | Probability is high because one of the super users of the system has done a crime that affects the company. |
| **Reputation & Customer Confidence** | 9 | Reputation of the company will be harmed and the customers’ confidence about the company will reduce in a comparatively high value. Because customers will not have any faith in the company as they have become the victims of a fraud. Therefore, a high value is given (9/10) |
| **Financial** | 7 | Financial loses will occur to the company. Because customers will be disappointed and afraid to trade with the company. Because of that the financial level of the company will reduce and company must put a lot of money to explore this issue as well as might cost money for resources for justifications and legal services. (If an customers take legal action against the company). Therefore, more than average value is given (7/10) |
| **Productivity** | 7 | Because customers disappointment they will be fearful to trade with the company. Because of that the sales will be decrease. Because of that the production will also decreases and the productivity of the company will automatically reduce.  Therefore, a high value is given (710) |
| **Safety & Health** | 0 | There is no impact on safety and health. Therefore, no value is given (0/10). |
| **Fines & Legal Penalties** | 6 | Since the fraud is an internal attack the chances of getting fines are high. There is a high probability for being charged with penalties for insufficient risk mitigation methods which leads to loss of customers’ sensitive details. Therefore, more than an average value is given (6/10) |
| **User defined Impact Area** | 0 | There are no User Defined Impact Areas. Therefore, no value is given (0/10) |

* 1. Justification of probability and Severity values of Risk Scenario 2

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Justification** |
| **Probability** | 75% | Probability is high because there is no backup to restore the legitimate data that has been modified which costs financially |
| **Reputation & Customer Confidence** | 7 | Reputation of the company will be harmed and the customers’ confidence about the company will reduce in a comparatively high value. As already the company doesn’t have a method to recover the legitimate data customers will no longer trade with the company.  Therefore a high value is given (7/10) |
| **Financial** | 5 | Financial loses will occur to the company. Because they must implement new SQL injection prevention methods and have to install a new backup system to the company to recover the original data that had been modified by the outsider. But this will be an advantage to the company in future needs. Therefore an average value is given (5/10) |
| **Productivity** | 7 | Because of not trading with the company, the sales will decrease. Hence the productivity of the company will be loss due to loss of sales. As well as the productivity of the employees might reduce due to additional tasks will introduce to employees due to prevention of the damage (installing a backup system and SQL Injection Prevention methods).  Therefore a high value is given (7/10) |
| **Safety & Health** | 0 | There is no impact on safety and health. Therefore, no value is given (0/10). |
| **Fines & Legal Penalties** | 5 | Since the fraud is an external attack the chances of getting fines are not high. But There is a high probability for being charged with penalties for insufficient risk mitigation methods which leads to modify details of the customer and others. Therefore, more than an average value is given (6/10) |
| **User defined Impact Area** | 0 | There are no User Defined Impact Areas. Therefore, no value is given (0/10) |

* 1. Justification of probability and Severity values of Risk Scenario 3

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Justification** |
| **Probability** | 75% | Probability is high because there are many DDoS attacks around. One person can control this type of attack and completely breaks a system temporally. |
| **Reputation & Customer Confidence** | 8 | When a DDOS attack happens to the system, reputation of the brand/ company will be damaged. As well as, because of DDOS attack confidential data will be lost. When customers’ confidential data loss, customers will be disappointed about the company and customers will lose their faith about the company.  Therefore, the high value is given (8/10) |
| **Financial** | 7 | Financial loses will occur to the customers as well as the company. Customers might lose their purchase details, outstanding details, customer reimbursement from the company from the attack and due to the legal processes company might have to bare the all lost if the company doesn’t have any recovery option.  Therefore, more than average value is given (7/10) |
| **Productivity** | 5 | This system is also use by the sales representatives of the company for invoicing. When the server gets down by the attack sales representative will not be able to reach the online platform for invoicing until the server restarts. Because of that the productivity of the employees will be decrease.  Therefore a high value is given (710) |
| **Safety & Health** | 0 | There is no impact on safety and health. Therefore, no value is given (0/10). |
| **Fines & Legal Penalties** | 3 | There is a probability for being charged with penalties for insufficient risk mitigation methods.  Therefore, more than an average value is given (6/10) |
| **User defined Impact Area** | 0 | There are no User Defined Impact Areas. Therefore, no value is given (0/10) |

* 1. Justification of probability and Severity values of Risk Scenario 4

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Justification** |
| **Probability** | 75% | Probability is high because the attacker has administrative privileges to the system. That means one person can control the full system as the administrator of the system. |
| **Reputation & Customer Confidence** | 8 | When outsider get administrative privileges to the system and he/she will access all the information including both sensitive data of the customers and the company. When the customers knowing about that attack, they will be disappointed about the company and they will be fearful to trade with the company and give their sensitive data such as bank details to the company. As well as the reputation of the company will be damaged.  Therefore, the high value is given (8/10) |
| **Financial** | 7 | The company will be responsible for investigating about this thread. Because of that company might spend huge amount of money on investigation.  Therefore, more than average value is given (7/10) |
| **Productivity** | 6 | Investigating about the attack will take excessive hours of effort. Because of that the productivity of the employees will decrease.  Therefore a the average value is given (6/10) |
| **Safety & Health** | 0 | There is no impact on safety and health. Therefore, no value is given (0/10). |
| **Fines & Legal Penalties** | 5 | There is a probability for being charged with penalties for insufficient risk mitigation methods.  Therefore, an average value is given (5/10) |
| **User defined Impact Area** | 0 | There are no User Defined Impact Areas. Therefore, no value is given (0/10) |

* 1. Justification of probability and Severity values of Risk Scenario 5

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Justification** |
| **Probability** | 75% | Probability is high because the attacker will encrypt all the data in the system and other important files in the computer |
| **Reputation & Customer Confidence** | 7 | When the attacker encrypts both sensitive data of the customers and the company as well as important files, they will be temporary unavailable for the system users. Because of that company will responsible for this issue. As a result of that customers will be disappointed, and the reputation will be damaged.  Therefore, the high value is given (7/10) |
| **Financial** | 8 | When the attacker encrypts the data by using encryption algorithms and he/she is the only person who knows the decryption passkey. So the company might be pay huge amount of money to the ransomware attacker in exchange of the necessary decryption passkey.  Therefore, the high value is given (8/10) |
| **Productivity** | 6 | When ransomware attack happens to the system/machines, they will not perform accordingly. The ransomware attack can damage of hostage systems, data, and files. Because of that employees will take lot of time to implement backup methods. As a result of that the productivity will be decrease. Therefore, more than an average value is given (6/10) |
| **Safety & Health** | 0 | There is no impact on safety and health. Therefore, no value is given (0/10). |
| **Fines & Legal Penalties** | 5 | There is a probability for being charged with penalties for insufficient risk mitigation methods.  Therefore, an average value is given (5/10) |
| **User defined Impact Area** | 0 | There are no User Defined Impact Areas. Therefore, no value is given (0/10) |

1. References

[1] – <https://www.idgconnect.com/idgconnect/opinion/1002869/common-causes-cloud-breaches>

[2] – <https://www.imperva.com/learn/application-security/syn-flood/>

[3] – <https://blog.mailfence.com/what-is-baiting-in-social-engineering/>

[4] – <https://blog.radware.com/security/2018/10/origin-of-ransomware/>

**Team Members Details**

|  |  |
| --- | --- |
| **IT Number** | **Name** |
| IT18085372 | V.K Maheswaran |
| IT18107692 | N.K Madanayake |