IT3070
Information Assurance and Security
3rd Year, 2nd Semester

Assignment

Submitted to

Sri Lanka Institute of Information Technology

IT18378658 - Perera A.P.A.D.

IT18153750 - Hearth H.M.R.K.R.

27/09/2020

Table of Contents

Introduction

We are considering the **Freedom Life Insurance Corporation** as our threat identified company. This is a newly started company in industry, and it has many facilities to do with technology. Technology based life insurance system is the main asset of the company and employees are working with many technology-based systems. Customers can do their task and everything with online platform provided by company. We are taking this as our selected company for identify critical threats using cyber security methodologies.

1.1 Change Information by Predators

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Insurance company details, Customer details
		Area of Concern	Change Information by Predators
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	Intruder will create company computer system security threats and malware. System security will be break through the internet and see company sensitive information and financial data. (Webroot)
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the company staff members should be able to access the data from the company system using company account's credentials. Customer details will be given under the legal permission.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** (75%) □ **Medium** (50%) □ **Low** (25%)
	(7) Consequences		(8) Severity

	What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	If customers detail and company details are modification, company has a huge risk. The company important information is lost, and the details cannot get back. Company has to put in a lot of money for get back this data. Customers cannot dicey this company for investment. The impact of negative feedbacks is cracked up the company brand name.	Reputation & Customer	8	6
		Financial	8	6
	When information of customers and Insurance company details lost, there will be a large drop down of company procedure. They need to work hard to recover lost data and re-think to make company new strategies because of the previous strategies data were lost.	Productivity	3	2.25
		Safety & Health	0	0
	If the company is ready to take legal actions, the company cannot find who has done it. Company has to bear a cost for find the predictors.	Fines & Legal Penalties	3	2.25
		User Defined Impact Area	0	0
			Relative Risk Score	16.5

(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?*		

Increase browser security settings (Webroot)	Monitor browser security settings every day and provide control level staff to configure browser issues.
Don’t open messages from unknown senders (Webroot)	Day to day email & other message resources filtering and giving proper idea to the users about unknown messages and share the details inside the organization.
Make secure and safety internet using process	There must be a proper documentation process about how safety Internet browsing for user reference. So, make secure every step of Internet browsing according to cyber security standard and give knowledge to company users in every level.
backup	If the company important details are lost by mistake or changed by someone, there will be arise a huge risk. Therefore, Maintain daily details (data) as a backup system. (E.g.: Cloud or physical device)

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high because of the attacker can do this task through the internet and do modifications to the data in current situation. So, this done by a human attacker, therefore it is very difficult to avoid the task. Therefore, there is a high probability for this risk.
Reputation & Customer Confidence	8	Reputation of the company is drop down because of this and there must be huge disappoint of customer confidence because of the customer data changing. Therefore, there will be a large customer dissatisfaction. Not only specified customers, all the customers are fall into this situation. Therefore, high value is given (8/10)
Financial	8	Financial loss will occur due to modification of company information and customer details. Then the company have to do rebuilt their strategies and plans in industry due to this attack. Sometime company have to pay compensations to the customers because of their information leaking. Therefore, high value is given (8/10)

Productivity	3	Some of the employees have to face this situation and they have to do their works again to success a company goal. Company productivity is not stable in current situation. This situation only effects some employees. Therefor a low value is given (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	3	Because of the outside attack there will be little release of legal side. They can add some fines for customer details are modification. The reason is not highly protect customer details as a company. Therefore, a low value is given (3/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.2 Man in the Middle(MitM) for online activities

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Customer’s credit card details, Company online payment service, Mobile Phone
		Area of Concern	Man in the Middle (MitM) for online activities
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	Intruder monitor when the customers are doing insurance payments through the company website using his online payment facility and using his mobile phone connecting to public network. Attacker monitor his activities between server and client, then he hijacks credit card information without customers’ consent.
		(3) Motive *What is the actor’s reason for doing it?*	Intentional (Fraud)

(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?*	Customers are doing insurance payment through the company online web page by using customer personal profile's valid credentials. Customer personal profiles cannot use unauthorized users.		
(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**
If customer's credit card is used, customer is not willing to use online services of the company for insurance payments. Company has to get financial risk of customers' losses. Company web site has weak authentication, customers give negative impact for the brand name.	Reputation & Customer	8	6
	Financial	5	3.75
To investigate the MitM attack which take more time to analyzing and finding the details. They have to get outsource help from third party peoples to investigate this.	Productivity	3	2.25
	Safety & Health	0	0
If the customers take legal actions against the insurance company, company has to bear a cost for get legal services.	Fines & Legal Penalties	8	6
	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?*
Restrict end user access to systems	Allocate only special users to access to the system with providing rules and regulation to their activities in the system.
Use running up-todate software	Many intruders target computer system and networks outdated software. Operating system and web browser and other software is up-to date to protect from internet related fraud.
Train how to use devices securely.	Attacker done middle attack with using server and user communication monitoring. So, with providing better guidance to the user how to work with devices securely is the way to avoid MitMs attacks.
Use OTP (One Time Password)	When the customer makes some payments, Company will provide One time Password.

Justification of probability and Severity values

Attribute	Value	Justification

(6) Probability	75%	Probability is high because of the company don’t use proper MitM avoid system to defend the MitM attacks. Therefore, there is a high possibility to affect that threat in every device information. Since the company is allowing to access every Website through the company Computers is another reason. With these faults the attacker can do attack easier to the devices. Therefore, threat probability is very high.
Reputation & Customer Confidence	8	Reputation of the company will be damaged and customer confidence are going down highly. Customer trust the company very strongly and with this incident of leaking customer credit card details occur the customer dissatisfaction on the company. It will highly affect to the company reputation and customer confidence. Therefore, a high value is given (8/10)
Financial	5	Financial loss will occur due to customer take legal action to this situation. Customer lost his trust on the company and company have to recover their losses in financial way. Therefore, a medium value is given (5/10)
Productivity	3	Productivity of the employees might be reduced because of the additional task is occurring with this situation. Then some employees have over working to recover this. Other employee can work normally because of this incident affect only few special employees. Therefore, a low value is given (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	8	Since the attack is an internal attack the chances of getting fines are high. If the customers take legal actions against the insurance company, company has to bear a cost for getting legal services. As well as there is huge possibility to pay fines and legal penalties for the details use of insecurely. Therefore, a high value is given (8/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.3 Malicious code attack (Virus)

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	**Threat**	Information Asset	Company hardware resources, company software		
		Area of Concern	Malicious code attack (virus)		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
		(2) Means *How would the actor do it? What would they do?*	Intruder sent malicious code as an email attachment or a download with the intent of infecting company computer. When the virus attached program is running in the company computer, it infects to the computer hard drive. Company system and programs are crashed. (get cybersafe)		
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)		
		(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 use security settings having web browsers to deal with internet. Staff members cannot download any software by own will without the company IT branch permission. Then intruder cannot reach easily to the company system.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **(75%)**	[✓ □ **Medium** **(50%)**]	□ **Low** **(25%)**
	(7) Consequences			(8) Severity *How severe are these consequences to the*	

	What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	If intruder effect to the company computer system, lot of recourses are crashed, and company have to bear huge amount of cost to reunion the resources. When programs are running without any control, company duties are drop down instantly. Even the company efficiency is also loss.	Reputation & Customer Confidence	6	3
		Financial	6	3
	With malicious attacks(viruses) effect to the hardware and some software. Therefore, it will take more time to rebuilt hardware and software to working level. Then some steps of day to day process still hold due to this situation.	Productivity	7	3.5
		Safety & Health	0	0
	If company get the legal actions, company have to bear a cost for hearing lawyers and legal matters.	Fines & Legal Penalties	2	1
		User Defined Impact Area	0	0
			Relative Risk Score	10.5

(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?*		
Avoid unknown mails and massagers. (Webroot)	Advising Users to work according anti malicious code software to avoid this threat. Always responsible for filter mails by using this software.		

Up-to date antivirus software. (Webroot)	When antivirus software is giving notification to update the version, the user must know to update the antivirus software instantly. IT technicians are responsible for set its' updates automatically.
Filter all emails. (bh consulting)	All incoming and outgoing (innovation work) emails should be filtered for prevent computer virus.
Provide Backup system	If the system is down, customers cannot do anything. Their work slows down. Therefore, there is a backup server for their very important transactions.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability is average since most of the browsers supports anti-virus and scam prevention tools and recommend users to work according to the antivirus software and rules and regulations. Therefore, it has 50% probability to occur this.
Reputation & Customer Confidence	6	Reputation of the company is high risk because of its affect to the company outside reputation. If the service is down/not working, reduce the customer's trust and confidence about the company. Therefore, a high value is given (6/10)
Financial	6	Financial loses will occur due to this situation. With malicious software attacks can affect to the hardware, So the company have to purchase new one and lot of money and time have to be spend to find this attack. Therefore, a high value is given. (6/10)
Productivity	7	When the devices are stopped working as a result of malicious codes also the working process is still holding due to devices are not working. So, the company process is going down with this activity. Low productivity is high risk to the company. Therefore, 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	2	Sometimes can add fines and legal penalties for the working at risk and added less value of (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.4 Steal restricted area devices and replace with fake devices.

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Company, company data resources
		Area of Concern	Steal data devices and replace fake devices
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	Intruder enter to the company without authority with an idea of steal valuable data devices from restricted area. Attacker steal a data device and replace it with a fake device like original one.
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)
		(4) Outcome *What would be the resulting effect on the information asset?*	[✓ □ **Disclosure**] □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Unauthorized persons cannot operate and use restricted area devices. The devices can be operated by company legal authorized operators only.
		(6) Probability	□ **High** [✓ □ **Medium**] □ **Low**

		What is the likelihood that this threat scenario could occur?	**(75%)**	**(50%)**	**(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**
If company restricted devices were stolen and replaced with fake devices, company has to face a huge risk of losing valuable devices and data. future goals' strategies and new projects are lost, and company cannot competitive with other companies. There is a Loss the company reputation.	Reputation & Customer	4	2
	Financial	9	4.5
Services of related to the restricted area devices are lost by without original data. There is a risk for the company safety.	Productivity	7	3.5
	Safety & Health	0	0
Fines and legal penalties are claim sometime due to low security protection and have to face legal action in this situation.	Fines & Legal Penalties	3	1.5
	User Defined Impact Area	0	0
		Relative Risk Score	11.5

(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	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		

you apply controls?	
Secure with a password, fingerprint, Facial recognition (Biometrics)	The restricted area devices are secure with a password. The devices data can get using a strong password. Using Biometrics (fingerprint, Facial recognition)
Use surveillance cameras	Surveillance cameras can detect potential threats as well as provide legal review after incidents.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability is medium because there are many ways to protect valuable data devices and storing rooms. But only one can access that area without permission with idea of steal a data device. Therefore, medium value probability can given.
Reputation & Customer Confidence	4	Company has low reputation damage because this is not related to working process. Only one person belongs to this task. Therefore, low value is given (4/10)
Financial	9	Financial loss will occur due to steal of original devices. Then the company have to re purchase them and company bear a cost to find a person who do that. Therefore, an high value is given (9/10)
Productivity	7	Productivity stops due to Data devices lost. All the devices store previous data and that are more useful for future works. Then the productivity is still stuck in some stages. Therefore, high value can given (7/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	3	Fines can add under not securely using devices. Then we can give low value (3/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.5 A virus goes through a device to the server by mistake.

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Company server, staff member’s computer
		Area of Concern	A virus goes through a device to the server by mistake.
		(1) Actor *Who would exploit the area of concern or threat?*	Company Staff member
		(2) Means *How would the actor do it? What would they do?*	Staff member’s machine has a virus. but he doesn’t know anything about it. if he connected the device to the server, A virus goes through a device to the server by mistake.
		(3) Motive *What is the actor’s reason for doing it?*	Accidental
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset’s security requirements be breached?*	Company staff members cannot access to connect their own devices. Instead of that company provides devices. Staff members cannot download any software by own will without the company IT branch permission.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **(75%)** □ **Medium** **(50%)** □ **Low** **(25%)**
	(7) Consequences		(8) Severity

	What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	Customer cannot check their details, transaction payments due to the server is down. If the service is down/not working, reduce the customer's trust and confidence about the company. After the virus goes to server, the virus can go to other devices as well. These devices can be damaged.	Reputation & Customer Confidence	6	3
		Financial	8	4
	With viruses effect to the hardware and some software. Therefore, it will take more time to rebuilt hardware and software to working level. Then some steps of day to day process still hold due to this situation.	Productivity	6	3
		Safety & Health	0	0
	If company take a legal action against to the staff member, company have to bear a cost for legal matters and waste to time for it.	Fines & Legal Penalties	2	1
		User Defined Impact Area	0	0
			Relative Risk Score	**11**

(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?*
Up-to date antivirus software. (Webroot)	When antivirus software is give notification to update the version, the user must know to update the antivirus software instantly. IT technicians are responsible for set its' updates automatically.

Provide Backup system	If the system is down, customers cannot do anything. Their work slows down. Therefore, there is a backup server for their very important transactions.
Confirm there is no virus	Check every device and make sure there is no virus inside the devices and server.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	When a device is connected to a server, the virus can go to other devices as well. Therefore, medium value probability can give.
Reputation & Customer Confidence	6	Reputation of the company is high risk because of its affect to the company/customers. If the Customer cannot check their details, transaction payments due to down the server, reduce the customer’s trust and confidence about the company. Therefore, a high value is given (6/10)
Financial	8	Financial loses will occur to the customer as well as the institute. After the virus goes to server, the virus can go to other devices as well. These devices can be damaged. Therefore, there can be a big damage. Therefore, a high value is given (8/10)
Productivity	6	When the devices are stopped working as a result of viruses also the working process is still holding due to devices are not working. So, the company process is going down with this activity. Low productivity is high risk to the company. Therefore, high 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	2	Sometime fines can be adding due to work with risky situation and without security option. Therefor a less impact value is given (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

References

bhconsulting. (n.d.). Retrieved from https://bhconsulting.ie/: https://bhconsulting.ie/computer-security-threatssolutions/

Webroot. (n.d.). Retrieved from www.webroot.com: https://www.webroot.com/us/en/resources/tipsarticles/computer-security-threats

Webroot. (n.d.). Retrieved from www.webroot.com: https://www.webroot.com/us/en/resources/tipsarticles/computer-security-threats-hackers