IT3010

Information Assurance and Security

3rd year 2nd Semester

Risk Management Assignment

Name	Registration No.
Siriwardana A.P.G.D. P	IT21345746
Hettiarachchi H.K.Y. K	IT21181474

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

01.10.2023

Table of Contents

1. Introduction

[4] Atlas Axillia Co (Pvt) Ltd. Is a leading stationary manufacturing company in Sri Lanka since 1959 September. It was started as the name Ceylon Pencil Company (Pvt) Ltd by Mr. D.S. Madanayake who was the first chairman of the company. By starting Pencils, they manufactured pens, color products and more stationary items.

In April 2017 they produced their first pencil after renaming themselves as Atlas Axillia Company (Pvt) Ltd.

Then in January 2018 they became a part of Hemas Holdings PLC. Due to their success, competitive companies tried to steal their position in the marketplace. When referring we find out some articles, regarding this. [5] Ada Derana, [3]Atlas and [6]Daily FT.

2. Allegro – Worksheet

2.1. Risk Scenario 1

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	The whole Atlas Axillias company			
	Area of Concern	*Targeted by hate campaigns*			
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Outsiders		
		(2) Means *How would the actor do it? What would they do?*	Misused the brand name and promoted hate speech and fake news among people. [1] children were asked to avoid using Atlas products.		
		(3) Motive *What is the actor's reason for doing it?*	To get short term competitive advantage		
		(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?*	Got legal actions and launched campaigns for reveal the truth.		
		(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**
[2] Try to get a market for low quality products	Reputation & Customer Confidence	9	6.75
	Financial	8	6
Reputation will be drop	Productivity	9	6.75
	Safety & Health	9	6.75
	Fines & Legal Penalties	9	6.75

		User Defined Impact Area	0	0
			Relative Risk Score	**33**

(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	[3]Took actions with CID
Launched campaigns	Launched campaigns for Trade, School and public for reveal the truth

2.2.Risk Scenario 2

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Employee Database		
	Area of Concern	*Destruction of Database*		
	(1) Actor *Who would exploit the area of concern or threat?*	Natural Disaster (No actor)		
	(2) Means *How would the actor do it? What would they do?*	The company's HR department is a particularly important location because it manages all the employee data. May be due to an unexpected high voltage power surge, a fire can be started, and the entire room catch fire and all the servers and databases will be destroyed.		
	(3) Motive *What is the actor's reason for doing it?*	Un-Intentional		
	(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?*	Do regular checkups in the HR department. Set up remote backups on cloud storage. Manage temperature using required effective system.		
	(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**
Huge damages for the valuable assets in the company due to fire and it losses financial benefits and losses valuable data.	Reputation & Customer Confidence	2	1
	Financial	8	4
Productivity will be temporarily drop.	Productivity	8	4
	Safety & Health	9	4.5

	May be end up with casualties.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	0	0
			Relative Risk Score	**16**

(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?*		
Manage the temperature and humidity	Because the assets in the HR department run continuously controlling the temperature and humidity is important. Temperature and humidity should be in moderate amount otherwise it will cause high heat, rust, corrosion etc.		
Use cloud backup storage	Regularly backups the database to cloud storage will keep the data safe and access it whenever needed.		
Use properly functioning UPS	To get redundant power supply in case of uninterrupted supply is used.		

2.3. Risk Scenario 3

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk — Threat	Information Asset	Research and development data		
	Area of Concern	*Insider Threat*		
	(1) Actor *Who would exploit the area of concern or threat?*	Insider		
	(2) Means *How would the actor do it? What would they do?*	Insider reveals the upcoming plans and ideas to outsider		
	(3) Motive *What is the actor's reason for doing it?*	For gain more money		
	(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?*	Staff members should be aware of their own responsibilities and not to reveal secrets for their personal victories.		
	(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**
Companies' reputation will be damaged.	Reputation & Customer Confidence	9	2.25
	Financial	0	0
Companies' trust in their employees will be decreased.	Productivity	5	1.25
	Safety & Health	9	2.25
Productivity issues.	Fines & Legal Penalties	7	1.75
	User Defined Impact Area	0	0

Relative Risk Score	7.5

(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?*
Introduce new rules and regulations	Give agreement to the employees for agree with rules and regulations in the company.

2.4.Risk Scenario 4

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Servers, Firewalls, Routers, and other networking equipment.			
	Area of Concern	*IT infrastructure and Network Security*			
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Insider or Outsider		
		(2) Means *How would the actor do it? What would they do?*	Occurs data traffic within network of the company (DDoS) causing disruption. Lack of Intrusion Detection Systems (IDS) allows intruders to access the network without knowing.		
		(3) Motive *What is the actor's reason for doing it?*	Competitors using DDoS attacks for competitive advantages by disrupting them. Delayed responses by intruders for complete their own purposes.		
		(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?*	Use required security tools and controls (Engage a DDoS mitigation service, Monitoring, and alerting)		
		(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**
Increases vulnerabilities causing wide range of cyber threats.	Reputation & Customer Confidence	0	0
	Financial	5	3.75
Productivity issues due to resource drain.	Productivity	9	6.75
	Safety & Health	9	6.75
	Fines & Legal Penalties	8	6

		User Defined Impact Area	0	0
			Relative Risk Score	**29.25**

(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?*
Rate limiting	Restrict the number of requests from single IP address
Implement traffic analysis tools	Monitor and analyze incoming traffic patterns to detect suspicious behaviors.
Engage a DDoS mitigation service	Capable of detecting and mitigating DDoS attacks in real-time.
User training	Held awareness sessions for the staff members.
Monitoring, and alerting	Monitor network traffics and establish alerting mechanism.
Network segmentation	Limits the potential damage from DDoS attacks

2.5.Risk Scenario 5

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Atlas Company's Product designs		
	Area of Concern	*Data Breach*		
	(1) Actor *Who would exploit the area of concern or threat?*	Outsider		
	(2) Means *How would the actor do it? What would they do?*	Companies are using some third parties (vendors, partners) for design their components since those kinds of vendors are lack of security intruder can easily get into them and steal the designs.		
	(3) Motive *What is the actor's reason for doing it?*	Intruder can be a person who hires from another competitive company with the mentioned company. So, copying the leading companies' designs will make their products looking good and since the designs are same people will deceive and buy them without any clarifications. Intruder can sell them to another party and earn money or intruder can blackmail the company and earn money as much as wanted.		
	(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?*	Hire faithful third parties for design purposes while getting agreement.		
	(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**
As a leading stationary company in Sri Lanka, the designs are unique to their own. If someone copies them	Reputation & Customer Confidence	7	5.25

	the designs will be the same, but the quality maybe not be as good as the original. When customers buy fake copies, they can feel the difference, so they think it's cheating. It will effect to the business of the Atlas company and their financial states because customers will not buy them even they are original, but the difference can't be identified by looking at them.	Financial	8	6
	If any intruder sells the designs to another party it's also the same and the uniqueness of the designs are no more valid. Anyone can copy them.	Productivity	0	0
		Safety & Health	7	5.25
	The intruder starts to blackmail and request money then the company must come up with legal action. They all have additional cost.	Fines & Legal Penalties	8	6
		User Defined Impact Area	0	0
			Relative Risk Score	**22.5**

(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?*		
Hire professional, responsible, and honest designers.	When hiring designers, company must consider their past experience and work history.		
Secure every device using necessary methods.	Give devices by company own and make sure they are secured with firewalls, passwords, Anti-virus etc.		

3. Appendix

3.1.Justification of Probability and Severity values of Risk Scenario 1

Attribute	Value	Justification
Probability	75%	Since Atlas Axillia is a leading stationary company in Sri Lanka, competitive companies trying to steal their marketplace and drop their reputation. So, it has high probability, and it was happened.
Reputation & Customer Confidence	9	As a Sri Lankan respective company, posting fake news about Atlas may cause customer dissatisfaction and they hesitate to trust. Then the company reputation will drop. Therefore, high impact value is given.
Financial	8	Customers are aware of getting products because they think its fake news are truth due to hate campaign. It affects their purchasing decisions and causes high impact value on finances.
Productivity	9	Due to fake news suppliers also confusing and refusing giving materials for their manufacturing purposes. It affects their high impact of productive.
Safety & Health	9	Hate campaigners misused Atlas brand name that is the main identity of their company. Then the marketplace in the industry for atlas companies is going to drop. It causes high impact value on company safety.
Fines & Legal Penalties	9	Due to misuse of their name and brand they took legal action with CID. It causes high impact value of Fines and Legal Penalties.
User Defined Impact Area	0	There is no user defined impact area.

3.2.Justification of Probability and Severity values of Risk Scenario 2

Attribute	Value	Justification
Probability	50%	May be due to an unexpected high voltage power surge, a fire can be started, and the entire HR department room catch fire and all the servers and databases will be destroyed. But it can happen very really. So, it has medium probability.
Reputation & Customer Confidence	2	May be due to an unexpected high voltage power surge, a fire can be started, and customers and employees may have displeasure about company risk management system. But it is a natural disaster and unavoidable, so it has low impact value.
Financial	8	Because of the fire valuable assert will be damaged. Too much cost for rebuilding the system again. So, finances have high impact value.
Productivity	8	Because of the fire valuable assert will be damaged and destroyed assert and system should rebuild again to get previous productivity as same as before. So, productivity have high impact value.
Safety & Health	9	May be end up with casualties. So, safety and health have high impact value.
Fines & Legal Penalties	5	If there are casualties, the family members can request for compensation and take legal actions against the company.
User Defined Impact Area	0	There is no user defined impact area.

3.3.Justification of Probability and Severity values of Risk Scenario 3

Attribute	Value	Justification
Probability	25%	Most employees are not going to do that because they are not willing to harm their company. So, Research and development data has low Probability of revealing company data to outsiders by insiders.
Reputation & Customer Confidence	9	Companies' trust and reputation in their employees will be decreased. Reputation & Customer Confidence has high impact value.
Financial	0	There are no financial issues.
Productivity	5	Due to giving secret and upcoming plans to outsiders, the company must take action to start again their plans and it is a time waste. So, it has medium impact value.
Safety & Health	9	Due to leaked upcoming plans of Atlas the future of the company will be damaged. Sometime company should take strict rules that may cause employees health, and safety problems so they will be tired of their job. So, Safety and Health has high impact value.
Fines & Legal Penalties	7	Due to giving secret documents and data to outsiders, the company must take legal action and fire the staff member who did the crime. So, it has high impact value.
User Defined Impact Area	0	There is no user defined impact area.

3.4.Justification of Probability and Severity values of Risk Scenario 4

Attribute	Value	Justification
Probability	75%	Assuming Atlas is more usage of networking infrastructures to manufacturing process, and database handling, etc. If someone is attacking the network may be a huge damage to the company. So, it has high probability.
Reputation & Customer Confidence	0	There are no reputation & customer confidence issues.
Financial	5	Intruders can change the financial data in the databases. When the network is restored, updating security systems make more cost. So, the impact given as medium value.
Productivity	9	Productivity issues due to resource drain. Productivity has high impact value.
Safety & Health	9	Increases vulnerabilities causing wide range of cyber threats may cause high impact of safety and health.
Fines & Legal Penalties	8	After monitoring and investigation of the attack the intruders can be found. It may be insider or outsider, if it is insider from the company according to the company rules and regulations necessary actions to be taken. Fines & Legal Penalties has high impact value.
User Defined Impact Area	0	There is no user defined impact area.

3.5.Justification of Probability and Severity values of Risk Scenario 5

Attribute	Value	Justification
Probability	75%	Since Atlas Axillia is a leading stationary company in Sri Lanka, competitive companies trying to copy their brand and build up their community. So, it has high probability
Reputation & Customer Confidence	7	Counterfeit copies can be the same, but their quality may not be the same as the original quality. It may cause customer dissatisfaction and they hesitate to buy. Then the company reputation will drop. Therefore, high impact value is given.
Financial	8	Customers are aware of getting products because they think its cheating due to low quality counterfeit products. It affects their purchasing decisions and causes high impact value on finances.
Productivity	0	There are no productivity issues.
Safety & Health	7	Intruders may blackmail or export stolen designs to other parties and will drop the uniqueness in the company. Then the marketplace in the industry for atlas company is going to loss. It causes high impact value on company safety.
Fines & Legal Penalties	8	Due to blackmail and copying their own brand by others the company must go to take legal action. Also, legal actions need to pay some cost.
User Defined Impact Area	0	There are no user defined impact areas.

4. References

[1] "Atlas Axillia," Atlas Axlliia, [Online]. Available: https://www.atlas.lk/our-story/. [Accessed 28 09 2023].

[2] "Ada Derana," [Online]. Available: https://bizenglish.adaderana.lk/atlas-takes-action-against-malicious-hate-campaign-on-social-media/. [Accessed 01 10 2023].

[3] "Atlas," Atlas Axillia, [Online]. Available: https://www.atlas.lk/2019/07/05/takes-action-against-malicious-hate-campaign-on-social-media/#:~:text=We%20have%20lodged%20a%20complaint%20with%20the%20CID%20and%20we%20will%20be%20sending%20a%20Letter%20of%20Demand%20to%20some%20of%20the%20individuals%20. [Accessed 01 10 2023].

[4] "Daily FT," Wijaya Newspapers Ltd., 2004. [Online]. Available: https://www.ft.lk/front-page/Atlas-bemoans-economic-impact-of-hate-campaigns/44-681337. [Accessed 30 09 2023].

[5] "Atlas Axillia," Atlas Axillia, [Online]. Available: https://www.atlas.lk/2019/07/05/takes-action-against-malicious-hate-campaign-on-social-media/#:~:text=Innovate%20to%20offer,into%20the%20country.%E2%80%9D. [Accessed 01 10 2023].

[6] "Atlas," Atlas Axillia, [Online]. Available: https://www.atlas.lk/2019/07/05/takes-action-against-malicious-hate-campaign-on-social-media/#:~:text=Innovate%20to%20offer,into%20the%20country.%E2%80%9D. [Accessed 01 10 2023].