Sri Lanka Institute of Information Technology

Risk Management Assignment

Information Assurance & Security – IT3070

3rd Year – 1st Semester

B.Sc. (Hons) in Information Technology

Student ID	Student Name
IT21284120	Rashmitha K.M.
IT21290060	Hemashi T.G.B.

Table of Contents

1. Introduction

Virtusa Corporation is a multinational provider of information technology services, offering digital engineering, technology, and communications services and products to businesses around the world in the financial services, healthcare, communications, media, entertainment, travel, manufacturing, and technology sectors. Virtusa offers clients in 25+ nations in 50+ locations across the world consulting services in digital transformation, AI, cloud computing, robotics, data analytics, and other areas of technology.

The largest delivery centers for Virtusa are in Hyderabad, Chennai, and Colombo. The company is headquartered in Southborough, Massachusetts, in the United States. For US$2 billion, Baring Private Equity Asia purchased the business in February 2021. Virtusa works alongside with its clients to help them re-imagine their business models and develop plans to protect and expand their operations through the introduction of innovative products and services, the creation of distinctive digital consumer experiences, the use of digital labor to increase operational efficiency, the development of operational and future IT platforms, as well as rationalizing and updating their current IT applications infrastructure. As a result of this, its clients are also able to drive business growth providing customers with digital-first experiences while streamlining and updating their IT application infrastructure to support the digital business transformation.

In our quest to research organizations for our IAS Project, we stumbled upon Virtusa Pvt Ltd, a company that seems to thrive in the face of high-risk situations. They appear to handle their risk management operations with remarkable success. Thus, we jointly decided to choose Virtusa Pvt Ltd as our focal organization and to investigate how they manage risk based on what we've learned in our IAS module.

During our research, we used a method called the Top-Down approach to figure out which assets are the most critical. This approach helped us rank these assets based on their importance. With this method, we were able to identify the most risky critical assets at the top of the list.

Additionally, through our research, we also found out about potential threats, the current practices being used (like changing usernames and passwords, and logging out), vulnerabilities, and the security requirements needed to protect these assets. This information is crucial for understanding how to safeguard the most important parts of the organization.

Based on our research's final findings, we were able to assess the risk of the most critical asset and pay particular attention to how likely these risks are to happen. We then suggested the best ways to respond to these risks, proposing appropriate countermeasure techniques. We also identified the most suitable control techniques and outlined our ideas on how to effectively manage and control risk based on the specific risks we uncovered.

2. Allegro worksheets

2.1 Phishing Attack

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk		Information Asset	Private Employee Information and Account Credentials		
		Area of Concern	*Phishing Attacks*		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
		(2) Means *How would the actor do it? What would they do?*	The attacker sends fraudulent mail while posing as a trustworthy contact. The user opens the email, clicks on the malicious link, or opens the attachment without realizing it. The attacker can then gain access to account credentials and private employee information.		
		(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?*	Only the employees should be able to access the data from their accounts using their user ID and password. Employee data, including personal information, should be handled with care. Don't grant permission to or access to every employee employed by this company. Make sure that your insurance and privacy agreements are in order in case the government decides to force someone to give up access. Fraudsters can easily take advantage of employees' money for their own needs if they have access to sensitive information about them. If sensitive employee data ends up in the wrong hands, it could lead to sizable financial losses.		
		(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 the intrusion changed anything in the employee's account. The company is not in charge of looking into the security threat or data breach that occurred. The business should be able to locate every fake user and fake ID account created by intruders, complete with information.	Reputation & Customer Confidence	5	3.75%
		Financial	4	3%
	Because it requires examining the evidence gathered through various channels and looking into the transactions that took place, investigating the attack may take some time. The investigation must be funded, which necessitates a special task team and the associated expenses. As a result, the organization's capacity and safety will be significantly impacted.	Productivity	0	0%
		Safety & Health	8	6%
	Personal information loss cannot be directly connected to a company. However, if any employee decides to accuse the business of theft and file a lawsuit, union services will require a lot of resources. (For hiring a lawyer, parking expenses, and time spent)	Fines & Legal Penalties	2	1.5%
		User Defined Impact Area	0	0%
			Relative Risk Score	**14.25%**

(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?*
Install a malicious web filter to prevent threats like spam and malware.	Employees should be encouraged to install a malicious web filter that can detect spam, blank senders, and other online threats. Phishing attacks won't occur while they are on the website as a result.
Install a web filter to prevent access to harmful websites.	The web filter technology inspects the requested website when a user searches for an online resource before answering the DNS query. Access will be permitted if the web filter determines that the website is secure. If a risky or questionable site is discovered during the scan, the web filtering technology will prevent access. This will protect you from phishing scams.
Download free anti-phishing add-ons.	Nowadays, most of browsers let you download add-ons that detect the telltale signs of a malicious website or warn you about well-known phishing websites. There is no reason not to install this on each corporate device since they are typically completely free.
Change passwords frequently.	If the user has online accounts, you should make it a habit to change their passwords frequently in order to stop an attacker from gaining unrestricted access. The additional layer of security provided by password rotation can stop ongoing attacks and keep potential attackers out because user accounts might have already been compromised without the user being aware of it.

Justification of Probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	The probability is high as a result of an unauthorized person finding and disclosing sensitive employee information to outside parties. Hackers, cybercriminals, state-sponsored hackers or maybe third parties. There will be a significant risk for employees if they develop as predicted. Additionally, it will have an impact on the company's reputation.
Reputation & Customer Confidence	4	The company's reputation is unaffected, but the employee retains a significant amount of power. Employees may lose trust and confidence in the company if a phishing attempt occurs as a result of the company failing to adequately warn them about it. They are held to a high standard of responsibility for their actions. As a result, a low value is given.
Financial	4	The corporation won't be the only one to suffer financial setbacks. Personnel are held to a high standard of accountability for their actions, despite the fact that the organization must be prepared to look into such situations. Consequently, a fair value is assigned.
Productivity	0	Productivity is unaffected. Therefore, no value is given (0/10).
Safety & Health	0	Safety & Health is unaffected. Therefore, no value is given (0/10).
Fines & Legal Penalties	2	Using firewalls and similar restrictions reduces the possibility of facing legal consequences. However, because there is a chance that a flaw will be found, a lower rating of (2/10) is given.
User Defined Impact Area	0	There is no impact on the User-Defined Impact Area. Therefore, no value is given. (0/10)

2.2 Unauthorized Wi-Fi access by company devices

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk / **Threat**	Information Asset	Public WIFI connections		
	Area of Concern	*Unauthorized access to business data.*		
	(1) Actor *Who would exploit the area of concern or threat?*	Unauthorized Staff		
	(2) Means *How would the actor do it? What would they do?*	Unauthorized users have full access to unprotected devices connected to the same network. The information sent over the internet can then be accessed by other users.		
	(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?*			
	(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**
The organization and its administrative board might suffer a financial loss if such an incident takes place. The cost will increase if he grants another employee access to the password and the data, and they use it without his or her knowledge.	Reputation & Customer Confidence	1	0.5%
	Financial	5	2.5%
	Productivity	5	2.5%
	Safety & Health	0	0%
Employees may access other corporate systems or steal employee data using this network. Because of this, the	Fines & Legal Penalties	2	1%

	business has the right to take legal action against those employees.	User Defined Impact Area	0	0%
			Relative Risk Score	**6.5%**

(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?*
Surveillance	Ensure that computers and systems used by the staff are secure. Utilize a security system for computers at all times. Additionally, a reliable method for tracking monthly expenses should exist.
Logs of network activities	Establish a dedicated team to oversee network usage and activity while enforcing bi-weekly password changes. This procedure enables swift detection and thwarts unauthorized network access.

Justification of Probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	It is highly likely to occur because it is so simple: if the professor leaves the room without logging out, anyone can connect to the computer and look up the passwords for secure networks.
Reputation & Customer Confidence	1	The security flaw will make workers lose faith in the company. Therefore, a less significant value is given. (1/10)
Financial	5	The company will suffer a minor financial loss as a result of the data expenses. As a result, an average value is offered. (5/10)
Productivity	5	It has no impact on the output. As a result, no value is provided. (5/10)
Safety & Health	0	There is no threat to one's safety or health. As a result, no value is provided. (0/10)
Fines & Legal Penalties	2	There is little effect on legal penalties because the company can take action against such employees and make them pay fines for causing disturbance. Thus, a lower impact value is assigned. (2/10)
User Defined Impact Area	0	Currently, there are no User Defined Impact Areas. As a result, no value is provided. (0/10)

2.3 SQL Injection

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Company Internal Database		
	Area of Concern	*SQL Injection*		
	(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
	(2) Means *How would the actor do it? What would they do?*	A Structured Query Language (SQL) injection attack happens when a hacker modifies a typical SQL query on a database-driven website. It is disseminated by injecting malicious code into a search box on a vulnerable website, which compels the server to reveal sensitive data. As a result, attackers can now view, modify, and delete database tables. As a result, the attacker may acquire administrative rights.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(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?*			
	(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?

If company account information is stolen, the institution is responsible for conducting an investigation to protect the business's reputation. The company might suffer sizable financial losses as a result. Unhappy employees will also damage the brand's reputation. If the company's website is always accessible, its reputation will improve.

If information from an employee's account is stolen, the company's reputation will suffer.

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	5	2.5%
Financial	5	2.5%

		Productivity	0	0%
		Safety & Health	0	0%
	Even though the company is not directly to blame for the theft of the company's information, taking legal action against the company may necessitate some payment for justifications and legal services. It is unlikely that you will be punished because this is an external attack.	Fines & Legal Penalties	4	2%
		User Defined Impact Area	0	0%
			Relative Risk Score	**7%**

(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?*
Queries with parameters	Using parameterized queries, a SQL statement can be pre-compiled so that extra arguments can be added after the statement has been executed. The database can now recognize and differentiate between input data and code because of this technique. By automatically quoting user input and ensuring that it has no bearing on the desired result, this coding technique defends against a SQL injection attack. Although PHP 5.1 introduces PHP Data Objects as a superior method of communicating with databases (PDO), MySQLi's extension does allow parameterized queries. PDO uses methods to make it easier to use parameterized queries.
Validation of Data	Validates the details that the user has given. Through the use of a validation mechanism, it controls user input.
Stored Methods	The developer must logically group one or more SQL statements together to create an execution plan for stored procedures. Statements may be automatically parameterized in subsequent executions. Simply put, it is a type of code that can be saved and used repeatedly. Instead of repeatedly entering the query, you can just call the saved procedure whenever you need to run it.

Justification of Probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	There are several controls when using company programs, and the likelihood of a SQL Injection is moderate. SQL injection attacks, also known as SQLi, alter SQL queries and inject malicious code into them by taking advantage of application flaws. Despite the precautions, there is a 50% chance of SQL Injection because it is one of the biggest security concerns.
Reputation & Customer Confidence	5	The company has procedures in place to reduce the chances of reputational harm, so a lower impact value is assigned. (5/10)
Financial	5	Both the organization and the employees would suffer financial losses. If the employee experiences financial losses as a result of the attack, the organization might be required by law to make up those losses. As a result, a score of 5/10 is considered average.
Productivity	0	The level of productivity is unaffected. Therefore, there is no assigned monetary value. (0/10)
Safety & Health	0	Safe & Healthy will not be affected. As a result, no value is assigned. (0/10)
Fines & Legal Penalties	4	Employee protests may slightly affect legal sanctions, and if a sufficient mitigation plan is not implemented, the company runs the risk of being fined. The company might not be able to completely control the risk because some risk mitigation techniques are time-consuming or expensive. As a result, a lower impact rating (4/10) is provided.
User Defined Impact Area	0	There are no User Defined Impact Areas. As a result, nothing of value is offered. (0/10)

2.4 DDoS Attack

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Virtusa Company Portal		
	Area of Concern	*If an attacker performs a DDoS attack the system would be break down.*		
	(1) Actor *Who would exploit the area of concern or threat?*	Outside Attacker		
	(2) Means *How would the actor do it? What would they do?*	These attacks are specifically carried out by hackers. Using botnets, they flood the target server with requests, causing it to become slow or crash. It makes a website take longer to load or keeps users from accessing the site.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(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?*			
	(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**
DDoS attacks have the potential to harm the business, its diverse data, and its confidential data in a variety of ways. It might be a situation that hurts the reputation of the business.	Reputation & Customer Confidence	6	4.5%
	Financial	7	5.25%
The productivity of the company is seriously threatened because the attacker has blocked access to company resources, project details information, and support services.	Productivity	6	4.5%
	Safety & Health	5	3.75%
The organization's security will be affected by this. A center is offered because doing so permits the attacker to	Fines & Legal Penalties	4	3%

	learn about the company's projects without endangering the attacker's health.	User Defined Impact Area	0	0%
			Relative Risk Score	**21%**

(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?*
Configure the network hardware on your system to withstand DDoS attacks.	To stop a DDoS attack, we can make a few simple hardware settings adjustments. You can prevent some ping- and DNS-based volumetric attacks, for example, by configuring your firewall or router to drop incoming ICMP packets or to block DNS responses coming from outside your network (by configuring UDP port 53 to be blocked).
Expand the bandwidth	Essentially, this means you must budget enough bandwidth to handle any traffic peaks caused by potential cyberattacks. Please keep in mind that DDOS attack mitigation does not require just increasing bandwidth.

Justification of Probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	The chances are very high. In the event that a DDOS attack is successful, the server may be completely crashed, making the company website (portal) inaccessible for a while. One person can control the botnets, temporarily making the system completely unusable.
Reputation & Customer Confidence	6	The company's reputation suffers as a result. The deactivation of the company website may cause customers and employees to lose faith in the veracity of the data there. In a similar vein, the client loses faith in the business. Consequently, a high impact value is provided. (6/10)
Financial	7	If such an attack takes place, it is crucial to engage professionals right away to address the issue. Thus, the high value is provided. (7/10)
Productivity	6	As a result, the organization's productivity declines. The result is a systemic failure. The inability of employees to learn about related projects. Consequently, productivity is impacted. Consequently, we assigned it a high value.
Safety & Health	5	The organization's security will be impacted by this. The attacker can use the center to learn about the company's projects, but it has no negative effects on one's health.
Fines & Legal Penalties	4	Utilize to learn If the site has been hacked, it should be investigated, and the hacker(s) should be held accountable through the legal system. The business must pay the price. As a result, a low value is given. (4/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. As a result, nothing of value is offered. (0/10)

2.5 Ransomware Attack

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Virtusa Client E-mails, Proposals, Projects, and Contracts		
	Area of Concern	*Ransomware Attacks*		
	(1) Actor *Who would exploit the area of concern or threat?*	Outside Attacker		
	(2) Means *How would the actor do it? What would they do?*	Malware can be used to gain access to client emails, client proposals, and client contracts. malware that prevents users from accessing their data or information systems unless a ransom is paid to an attacker to unlock them.		
	(3) Motive *What is the actor's reason for doing it?*	The organizations or the attackers desire to earn ransom money.		
	(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?*			
	(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**
Anyone can use the system. Users may not use it. can harm a company's reputation and possibly even result in extortion.	Reputation & Customer Confidence	8	6%
	Financial	9	6.75%
Due to the company crash, employees cannot work with encrypted data.	Productivity	10	7.5%
	Safety & Health	0	0%
	Fines & Legal Penalties	8	6%

	An exclusivity agreement is broken if the attacker makes the data public. The impacted client may file a lawsuit against the company.	User Defined Impact Area	0	0%
			Relative Risk Score	**26.25%**

(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?*
Implement Anti-virus software	Responsible for updating anti-virus software. To receive updates, connect frequently to the Virtusa network. We use and keep up with the best antivirus software. • Conduct routine computer scans. • Enable firewall
Maintain Backups	Backing up important data is the most effective way to recover from a ransomware infestation. So that hackers cannot target your backup data, it should be properly protected and kept offline or out-of-band. Make sure to evaluate backup performance on a regular basis.

Justification of Probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	The possibilities that a ransomware attack will completely crash the server and cause the company's websites unavailable is very high. As a result, client emails cannot be accessed. Because of this, the pertinent project cannot be finished by the deadline set for today. Consequently, this has been given a high value.
Reputation & Customer Confidence	8	The reputation of the business will be damaged as a result. The confidence of both customers and employees in the privacy of customer information may be damaged. Thus, this will have an impact on the trust there. This is the rationale behind providing more value.
Financial	9	The customer may file a legal actions against the attacker if it refuses to release the data. It has been valued at a rather high amount.
Productivity	10	Being unable to access client emails prevents the organization from completing related projects on time, which has a negative impact on productivity. Consequently, this has been given more value.
Safety & Health	0	There is no threat to one's safety or health. As a result, no value is provided. (0/10)
Fines & Legal Penalties	8	The customer may file a lawsuit against the attacker if it refuses to release the data. It has been valued at a rather high amount.
User Defined Impact Area	0	There are no User Defined Impact Areas. As a result, nothing of value is offered. (0/10)

3. References

[1] R. Brooks, "netwrix blog," 06 04 2020. [Online].
Available:

https://blog.netwrix.com/2020/04/07/risk-analysis-example/

[2] Phishing attack

https://www.phishing.org/what-is-phishing

[3] University of Pittsburgh Information Technology "Disclosure of Sensitive Information"

https://www.technology.pitt.edu/security/disclosure-sensitive-information

[4] Brute-force attack - definition

https://www.kaspersky.com/resource-center/definitions/brute-force-attack

[5] Ransomware

https://security.berkeley.edu/faq/ransomware/

[6] Virtusa

https://en.wikipedia.org/wiki/Virtusa

https://www.virtusa.com/