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

Assignment

IAS 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

08/09/2019

AG UNIVERSITY OF TECHNOLOGY

Group Members

1) IT17077248 - Ranepura H.G.A.L
2) IT17100762 – Jayapadma J.H.M.A.C

1. Student personal data breach

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Student Details		
	Area of Concern	Student personal data breach		
	(1) Actor *Who would exploit the area of concern or threat?*	Internal staff member		
	(2) Means *How would the actor do it? What would they do?*	Internal staff member who might or might not aware of the organization's rules and compliances might expose sensitive data of a student, which is also referred to as insider data to a third party.		
	(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?*	Students' personal data should only be accessed by the relevant administrative staff of university. Sensitive data of the student such as student contact information, marks, transaction, log etc., in the wrong hands can cause major loses for university and student.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	❑ **Medium**	❑ **Low**

(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**
Student personal data is leaked, University is responsible of investigating it to protect the repudiation of the university. This might bring massive financial losses to the university because decreased the income of university. And also, it can cause to student life. Student will be disappointed and the discouraged to enter the university for	Reputation & Customer Confidence	8	6
	Financial	5	3.75

	his students, which will finally lead to a negative impact on the university name and rank.			
	Investigating the data breach might take excessive hours of specific system, a special task force might be needed for the investigation and the cost of it will be high.	Productivity	3	2.25
		Safety & Health	0	0
	If the student take legal actions against the University, even though the administrative staff's action was not intentional for the theft of their data, it might cost some amount of resources for justifications and legal services (example – Hiring Lawyers)	Fines & Legal Penalties	6	4.5
		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?*
Conduct workshops, awareness sessions and conferences	The administrative staff should be given a proper induction on data security and its risk. Even after the initial training sessions it is important to keep the administrative staff updated about the possible attacks and new risks.
Surveillance	University internal and external audits on all the communication channels and other data transformation methods frequently. Restrict inappropriate files sharing with external parties examples - set limits for the shareable files size, control external mail channels
Set standards	Set internal standards for student information managements inside the University. Create timely compliance documents and update the existing agreements, rules and regulations with the administrative staff, about internal data security.
Share Experience	The past and present experience should be properly documented with evidence for future reference. Sharing the Risk experience will help the institutions to increase the security in the future and to improve the process.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	. Probability is high because the University is not checking the outside emails sent by the employees of the company. Since sending emails to outside of the organization cannot be controlled. Monitoring tools to check on the size and content of the emails is not implemented at the moment and staff can use external devices such as flash drives to copy data from their computers. Additionally, administrative staff are allowed to use cloud data storages (example – Google drive) and also personal emails and social media. Since the controls are less, there is a high probability for this risk.
Reputation & Customer Confidence	8	Reputation of the university will be damaged and the customer confidence about the university will reduce in a high rate, since students believe that their personal information is safe but failure to do so will reduce their confidence on the university. Students might lose their confidence in entering the courses. Therefor a high value is given (8/10)
Financial	5	Financial loses will occur to the university if the student is aware of the breech and if the student takes a legal action against the university. University might lose their trust and due to the legal processes institute might have to recover the students loses. Therefore, a medium value is given (5/10)
Productivity	3	Productivity of the administrative staff of the students might reduce due to additional task arouse due to investigation and prevention of the damage. However, the impact on productivity is for a short time. Once the solution and possible controls are identified the productivity of the staff will go back to a stable state. 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	6	Since the attack is an internal attack the chances of getting fines are high. There is a possibility for being charged with penalties for insufficient risk mitigation methods which leads to loss of students data. The company might have to pay lawyer fees, law court fines and also penalties for the students. Therefore, a high value is given (6/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

2. DDoS Attacks using Botnets

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Students Results DB
		Area of Concern	DDoS Attacks using Botnets
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder(Student) who uses Botnets
		(2) Means *How would the actor do it? What would they do?*	Botnets are group of computers with installed malware and showing malware behavior. These are controlled by hackers in large amounts to attack a server and stopping the service provided by it. These are also designed to steal data, and some are in form of ransomware. These are self-propagating and keeps continuously attacking a server pointed. These botnets request to the same service at single time and make the service incapable of providing response at once. Hence server stops, that's called Denial of service attack or DDoS attack. When the attacker attack to the students Results DB of university and attacker can steal the data.
		(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?*	Students' personal data should only be accessed by the lectures of university. When attacked to the student results DB, it going to failure. Then attacker can steal the data also. These data can be related to the upcoming releasing of the results. Whole year's results want to calculate GPA, pass rate, summary of results, identify repeat students, organize the repeat exams etc. So, when attacker down the DB can change and steal results. And also student can't be access to their results sheets. It is a major loss for the University.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	❑ **Medium**	❑ **Low**

(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 university DBs have weak authentications or incorrectly configured auth flows, botnets may crack the vulnerability and data will be bleached. If happens, university should be responsible for loss of student data.	Reputation & Customer Confidence	8	6
	Financial	5	3.75
Under GDPR regulations university have to pay a fine after estimating the type of attack (DDoS attacks are 3 types; volumetric attacks, application attacks, protocols attacks) and its damage.	Productivity	7	5.25
	Safety & Health	0	0
Students and Lectures won't able to see their results. Hence university will be lost it reputation due to loss of productivity.	Fines & Legal Penalties	4	3
	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?*
Buy more bandwidth	This enables the server to handle spikes in traffic. This traffic may be due to actual legitimate user increase or malicious botnet networks. By the way if the server has more bandwidth it will be able to handle the TPS (Transactions per second).
Network Traffic Analyzer with spike detection.	This enables the university to identify DDoS attacks to server. Perfect monitoring system can clearly separate an actual user from a botnet. Human intervention is also highly needed to monitor this traffic and mitigate immediately once detected. So, Network engineers need to be engaged in this work 24*7.
API throttling	Throttling is done to limit the request count and set permissions on requests to validate the API request to check whether it's valid or not. You can define this API level as well as application level.
Set Concurrent Connections Limit	This will automatically control DDoS attacks. This sets amount of pool for users. It can be configured region wise, IP wise etc. This will mitigate DDoS attacks automatically.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	. Probability is high because there are many DDoS attacks around and cost for initiating this type of attack is very low. One person can control botnets and completely breaks a system temporally.

Reputation & Customer Confidence	8	Reputation of the university will be highly damaged. Due to the down time of results DB, student will lose the faith about their result sheet system. Therefore, the high impact value is given (8/10)
Financial	5	Financial loses will occur to the University. University might have to recover the students loses. Therefore, an average value is given (5/10)
Productivity	7	Productivity of the university application goes down with this. This will result in complete student results DB failure. No one will be able to get their results and any results related activities until it fixed. There for the impact on productivity is high (7/10)
Safety & Health	0	There is no impact on safety and health. Therefore value is (0/10)
Fines & Legal Penalties	4	University might be fined under GDPR for data breach. Therefore, a medium value is given (4/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore value is (0/10)

3. Self-Service student payment machine skimming

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Student Card, Student payment machine
		Area of Concern	Self-Service student payment machine skimming
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder (Student)
		(2) Means *How would the actor do it? What would they do?*	Intruder will fix external devices to the Self-Service Student card machine and skim the data from the

			cards when students enter it to the machine and also record the password when the student types it in the key board using a hidden camera. Then intruder get payment details like payment id, amount, bank account details, etc. and change them as he wants.		
		(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 owner of the student card should be able to login the system to do semester and other payments using the student card. When intruder log to the system stele the payments and bank account details and change it and put the details to another login. So, actual payments change and mark as not payed. And also use the account details for their payments.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	❑ **Medium**	❑ **Low**

(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 details from students' login are stolen and change payments method, university is responsible of investigating and giving the payments back to protect the reputation of the bank. This might bring massive financial losses to the university. In addition to that, university will be disappointed and be discouraged to use student card service, which will finally lead to a negative impact on the university name	Reputation & Customer Confidence	3	2.25
	Financial	5	3.75
Investigating the crime might take excessive hours of effort, analyzing the evidence gathered through CCTV and analyzing the transactions happened. A special task force might be needed for the investigation and the cost of it will be high	Productivity	3	2.25
	Safety & Health	0	0

	If the customers take legal actions against the university, even though the university is not directly responsible for the theft of their payments, it might cost some amount of resources for justifications and legal services (example – Hiring Lawyers)	Fines & Legal Penalties	2	1.5
		User Defined Impact Area	0	0
			Relative Risk Score	**9.75**

(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?*
Break the single authority processes.	Rotate the Self-Service machine hardware providers, which will ensure that just one person will not handle the operations exclusively for a machine over a specified point.
Surveillance	Organize student card payment audit programs where machines will be randomly inspected onsite and also acknowledge the security officers as well as the student to report any unusual devices or people immediately.
Set standards	After installing the Self-Service machine hardware and software there should be proper documentation and visual presentation (photographs) ready to be crosschecked whenever a suspicious device is been identified.
Share Experience	The past and present experience should be properly documented with evidence for future reference. Sharing the Risk experience will help the institutions to increase the security in the future and to improve the process.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	. Probability is high because the attackers has been successful in replicating the same appearance to the trackers enabled devices. Since it is a physical attack and currently there are less controls the chances of attack is high.
Reputation & Customer Confidence	3	Reputation of the university will be damaged and the student confidence about the university will reduce in a comparatively low value since this will affect only to a specific section of students (Student card users). Students might lose their confidence in using student cards, but the reputation of the university will highly unlikely to be fully damaged. Therefor a low value is given (3/10)
Financial	5	Financial loses will occur to the student as well as the institute. Students might lose their payments from the attack and due to the legal processes institute might have to recover the student loses. Therefore, an average value is given (5/10)
Productivity	3	Productivity of the employees of the students might reduce due to additional task arouse due to investigation and prevention of the damage. However, the impact on productivity is for a short time. Once the solution is identified the productivity of the employees will go back to a stable state. Therefor a low value is given (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore value is (0/10)
Fines & Legal Penalties	2	Since the attack is an external attack the chances of getting fines are less. There is a possibility for being charged with penalties for insufficient risk mitigation methods which leads to loss of money from student's account. Therefore, a low value is given (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore value is (0/10)

4. Phishing attacks

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Course materials		
		Area of Concern	Phishing attacks		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder(Student)		
		(2) Means *How would the actor do it? What would they do?*	Intruder will create an exactly similar User interface to the University application. Then this will be sent via emails as advertisements, scholarships, or paying links. (Spams). When user clicks on these links and tried to log in, Intruder gets all the sensitive information students entered on that fake user interface. This may be student's Registration number, password, name etc. Intruder keeps collecting information like these. So afterwards intruder can logged in to these accounts using steal credentials.		
		(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?*	By having student's sensitive account details intruder can easily impersonate to be the students for his/her benefit. Student's account login data should only be accessed by the relevant administrative staff in the university. Sensitive data of the students, in the wrong hands can cause steal of course materials for use them to teach same lecture slides in another university and to know the standards of course materials.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	✓ **Low**
	(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
	This might bring financial losses to the university because fixed the attack and prepare and change the course materials again.	Reputation & Customer Confidence	0	0
		Financial	5	1.25
		Productivity	0	0
		Safety & Health	0	0
		Fines & Legal Penalties	0	0
		User Defined Impact Area	0	0
			Relative Risk Score	**1.25**

(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?*
Keep students informed about the phishing attack types	New phishing scams are being developed all the time and it is important to keep information about those up to date. The risks of different phishing scams should be informed to the students whenever possible.
Install an Anti-Phishing Toolbars	Advising the students to Install an Anti-Phishing Tools will control the phishing attacks that can happen to the students. If the students uses a malicious site those tools will give warnings before student clicks on any of the links available in the fraud sites.
Changing Passwords	Students should be advised to get into the habit of changing their passwords regularly. Even if the student is not following the requested good practices, university can reset the student passwords and ask them to create new passwords every 6 months or depending on university's choice.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	25%	. Probability is average since most of the browsers supports anti-virus and scam prevention tools and recommend students to use when they login to a application. But there are students who are not aware of using the tools and not aware of the risks, therefore a medium chance of a phishing attack is there.
Reputation & Customer Confidence	0	There is no impact on reputation & customer Confidence. Therefore value is (0/10)
Financial	5	Financial loses will occur to the university because fixed the attack and prepare and change the course materials again immediately.
Productivity	0	There is no impact on productivity. Therefore value is (0/10)
Safety & Health	0	There is no impact on safety and health. Therefore value is (0/10)
Fines & Legal Penalties	0	There is no impact on fines & Legal penalties. Therefore value is (0/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore value is (0/10)

5. AI-powered Attacks

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Administrative staff and student details, University details, Secret details (financial)		
		Area of Concern	AI-powered attack		
		(1) Actor *Who would exploit the area of concern or threat?*	AI- device or software		
		(2) Means *How would the actor do it? What would they do?*	The concept of a computer program learning by itself, building knowledge, and getting more sophisticated may be scary. Artificial intelligence can be easily dismissed as another tech buzzword. However, it is already being employed in everyday applications through an algorithmic process referred to as machine learning. Machine learning software is aimed at training a computer to perform particular tasks on its own		
		(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?*	This makes cyber-attacks such as identities, passwords and other secret details stealing or cracking and destroying.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	✓ **Medium**	❑ **Low**

(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**
It can be missing and destroy the financial details and other valuable things such as the certifications, credits etc. of university. Then the position (status) and identity of the university can be loss.	Reputation & Customer Confidence	8	4
	Financial	7	3.5
Under that kind of situations the works and duties of university are dimidiated. Whole system may be crashed.	Productivity	8	4
	Safety & Health	0	0

	Administrative staff and students can't access the websites furthermore. Because those are not secure under that situation.	Fines & Legal Penalties	3	1.5
		User Defined Impact Area	0	0
			Relative Risk Score	**13**

(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?*
Check all of the systems and devices in under the control	Check all devices, networks and confirm they are under control. This can be done by daily, weekly or monthly etc. And that decision about the period must be given by the causes of number of devices, number of networks etc.
Changing Passwords	Get backups of all valuable details of the university. And store them in high secure storages out of the university. Those storages must not related anyway of the other storages. And also that details must store a cloud database (google drive etc.)

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	. Probability is medium because this makes cyber-attacks such as identities, passwords and other secret details stealing or cracking and destroying.
Reputation & Customer Confidence	8	Reputation of the university will be highly damaged. Due to the down time of website, all activities of university failure(8/10)

Financial	7	Financial loses will occur to the university because they should fixed the attacks and due to down time all activities of university failure, So decrease the income.
Productivity	8	When all activities of university get down, decrease the productivity.
Safety & Health	0	There is no impact on safety and health. Therefore value is (0/10)
Fines & Legal Penalties	3	Administrative staff and students can't access the websites furthermore. Because those are not secure under that situation.
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore value is (0/10)