SECOM CASE STUDY

MANAGING INFORMATION SECURITY IN A RISKY WORLD

ISTM 635 – 603

SUBMITTED BY

SANDHEEP SRIDAR

Contents

Estimating CUSTOMER and EMPLOYEE servers

Customer and Employee server holds sensitive information of 600,000 registered users and 20 employees of Jashopper. This section aims to calculate the asset value of the aforementioned servers by pointing out specific evidence from the case.

The below table estimates the asset value of the customer server as 5330728.09 Yen and the Employee Server as 29928810 Yen.

Asset Value Estimate			Financial Impact		
Critical Assets	**Valuation Criteria**	**Number of Accounts**	**Average Value [AV Table]**	**Other Financial Impacts**	**AV**
Customer Server	Compensation to affected registered users	600,000	¥8.88	¥0.89	**¥5,330,728.09**
Employee Server	Compensation to affected employees	20	¥49,240.50	¥28,944,000.00	**¥29,928,810.00**

Specific Evidence, justification and calculation

The Exhibit 5 in the case depicts the financial impact of data breach incidents of 3 companies namely Softbank, kukaku.com and Uji Municipal Office. However, only kukaku.com was attacked by outsiders. The data provided for kukaku.com specifies that the sales and countermeasures costed them 200 million Yen for 22,511 users. For calculation of asset value of the customer and employee servers, we are only considering the data provided for kukaku.com as it depicts the impact of threat from outsiders.

For calculating the asset value, Morrison's compensation values were used as benchmark to calculate the financial impact on Jashopper (Refer the appendices section for calculations and references section for data source)

Estimating EF

Exposure factor is used to calculate the potential loss that is incurred if a threat becomes a reality. In this case, there are two important assets Customer and employee and for further calculations we assume that the EF value is 1. An EF value of 1 means that a complete loss of the asset has occurred.

Specific Evidence, justification and calculation

The Exhibit 7 in the case represents major information breaching incidents and all the incidents point to a major loss of assets and hence, we are assuming that any breach from outsider threat will have total impact on the Jashopper assets.

Estimate of SLE, ARO, ALE

In order to calculate cost of controls, the single loss expectancy, Annual rate of occurrence and Annual loss expectancy is calculated. For calculating these values let us consider the below threat statement

"Customer/Employee data stolen by an outside hacker"

SLE estimate

Single Loss Estimate is the product of Asset Value and Exposure Factor. We calculated the Asset value for customer and employee servers in the first section and we are assuming exposure factor to be 1. The following table depicts the SLE calculation for Jashopper assets:

		Assumption	SLE = AV * EF		
Asset	**Asset Value (AV)**	**Exposure Factor (EF)**	**Single Loss Expectancy (SLE)**	**Vulnerability**	**Threat**
Customer Personal data	¥ 5,330,728.09	1	¥ 5,330,728.09	Non Technical	Insider
	¥ 5,330,728.09	1	¥ 5,330,728.09	Non-Technical Human Error	Human
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Human Error	Human
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Vulnerabilities	Hackers
Employee Personal data	¥ 29,928,810.00	1	¥ 29,928,810.00	Non Technical	Insider
	¥ 29,928,810.00	1	¥ 29,928,810.00	Non-Technical Human Error	Human
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Human Error	Human
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Vulnerabilities	Hackers

ARO estimate

Annual rate of occurrence is the number of times data breaches happen in Jashopper's assets.

Asset	**Vulnerability**	**Threat Agent**	**Annual Rate of Occurance (ARO)**	**NOTES**
Customer Personal Data Lost or Stolen	Non Technical	Insider	**25.00%**	Exhibit 4a
	Non-Technical Human Error	Human	**24.30%**	Exhibit 4a
	Technical Human Error	Human	**22.10%**	Exhibit 4a
	Technical Vulnerabilities	Hackers	**20.00%**	Exhibit 4a
Employee Personal Data Lost or Stolen	Non Technical	Insider	**20.00%**	Exhibit 4a
	Non-Technical Human Error	Human	**19.30%**	Exhibit 4a
	Technical Human Error	Human	**17.10%**	Exhibit 4a
	Technical Vulnerabilities	Hackers	**15.00%**	Exhibit 4a

The calculation of ARO for each vulnerabilities and its related threat is elaborated in the appendix section. The values were deduced from the exhibit 4a and 4b of the case.

ALE estimate

ALE is Annual Loss Expectancy and it is the product of SLE and ARO. The below table shows the ALE before any cybersecurity controls were applied.

		Assumption	SLE = AV * EF			[Source of Data]	ALE=SLE*ARO
Asset	**Asset Value (AV)**	**Exposure Factor (EF)**	**Single Loss Expectancy (SLE)**	**Vulnerability**	**Threat**	**Annual Rate of Occurance (ARO)**	**Annual Loss Expectancy (ALE)**
Customer Personal data	¥ 5,330,728.09	1	¥ 5,330,728.09	Non Technical	Insider	**0.250**	¥ 1,332,682.02
	¥ 5,330,728.09	1	¥ 5,330,728.09	Non-Technical Human Error	Human	**0.243**	¥ 1,295,366.93
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Human Error	Human	**0.221**	¥ 1,178,090.91
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Vulnerabilities	Hackers	**0.200**	¥ 1,066,145.62
Employee Personal data	¥ 29,928,810.00	1	¥ 29,928,810.00	Non Technical	Insider	**0.200**	¥ 5,985,762.00
	¥ 29,928,810.00	1	¥ 29,928,810.00	Non-Technical Human Error	Human	**0.193**	¥ 5,776,260.33
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Human Error	Human	**0.171**	¥ 5,117,826.51
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Vulnerabilities	Hackers	**0.150**	¥ 4,489,321.50
						TOTAL ALE	**¥ 26,241,455.81**

The ALE before applying cyber security controls is **26241455.81 Yen.**

Recommendation

ALE value after using solution A

Asset	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Vulnerability	Threat	Annual Rate of Occurance (ARO)	Annual Loss Expectancy (ALE)
Customer Personal data	¥ 5,330,728.09	1	¥ 5,330,728.09	Non Technical	Insider	**0.150**	¥ 799,609.21
	¥ 5,330,728.09	1	¥ 5,330,728.09	Non-Technical Human Error	Human	**0.170**	¥ 906,756.85
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Human Error	Human	**0.133**	¥ 706,854.54
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Vulnerabilities	Hackers	**0.120**	¥ 639,687.37
Employee Personal data	¥ 29,928,810.00	1	¥ 29,928,810.00	Non Technical	Insider	**0.120**	¥ 3,591,457.20
	¥ 29,928,810.00	1	¥ 29,928,810.00	Non-Technical Human Error	Human	**0.135**	¥ 4,043,382.23
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Human Error	Human	**0.103**	¥ 3,070,695.91
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Vulnerabilities	Hackers	**0.090**	¥ 2,693,592.90
						TOTAL ALE	**¥ 16,452,036.21**

The ALE value after applying solution A is **16452036.21 Yen**

ALE value after using solution B

Asset	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Vulnerability	Threat	Annual Rate of Occurance (ARO)	Annual Loss Expectancy (ALE)
Customer Personal data	¥ 5,330,728.09	1	¥ 5,330,728.09	Non Technical	Insider	**0.125**	¥ 666,341.01
	¥ 5,330,728.09	1	¥ 5,330,728.09	Non-Technical Human Error	Human	**0.122**	¥ 647,683.46
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Human Error	Human	**0.099**	¥ 530,140.91
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Vulnerabilities	Hackers	**0.090**	¥ 479,765.53
Employee Personal data	¥ 29,928,810.00	1	¥ 29,928,810.00	Non Technical	Insider	**0.100**	¥ 2,992,881.00
	¥ 29,928,810.00	1	¥ 29,928,810.00	Non-Technical Human Error	Human	**0.097**	¥ 2,888,130.17
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Human Error	Human	**0.077**	¥ 2,303,021.93
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Vulnerabilities	Hackers	**0.068**	¥ 2,020,194.68
						TOTAL ALE	**¥ 12,528,158.68**

The ALE value after applying solution B is **12528158.68 Yen**

ALE value after using solution C

Asset	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Vulnerability	Threat	Annual Rate of Occurance (ARO)	Annual Loss Expectancy (ALE)
Customer Personal data	¥ 5,330,728.09	1	¥ 5,330,728.09	Non Technical	Insider	**0.100**	¥ 533,072.81
	¥ 5,330,728.09	1	¥ 5,330,728.09	Non-Technical Human Error	Human	**0.097**	¥ 518,146.77
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Human Error	Human	**0.088**	¥ 471,236.36
	¥ 5,330,728.09	1	¥ 5,330,728.09	Technical Vulnerabilities	Hackers	**0.080**	¥ 426,458.25
Employee Personal data	¥ 29,928,810.00	1	¥ 29,928,810.00	Non Technical	Insider	**0.080**	¥ 2,394,304.80
	¥ 29,928,810.00	1	¥ 29,928,810.00	Non-Technical Human Error	Human	**0.077**	¥ 2,310,504.13
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Human Error	Human	**0.068**	¥ 2,047,130.60
	¥ 29,928,810.00	1	¥ 29,928,810.00	Technical Vulnerabilities	Hackers	**0.060**	¥ 1,795,728.60
						TOTAL ALE	**¥ 10,496,582.33**

The ALE value after applying solution C is **10496582.33 Yen**

Recommendation: The below table consolidates the calculations of ALE after applying all possible solutions and compares with other solutions. After analyzing the below data, I would recommend Jashopper to apply the **solution C** as it provides the highest net risk reduction benefit among all the solutions.

Parameter/Solution	A	B	C
Cost of Solution	3900000	6420000	6920000
Gross Risk Reduction Benefit (GRRB)	9789420	13713297	15744873
Net Risk Reduction Benefit (NRRB)	5889420	7293297	8824873
Is NRRB > 0?	YES	YES	YES

Would the above recommendation change if the company files IPO?

My recommendation would not change if the company is planning to go public. Cybersecurity readiness is an important issue for companies which are filing IPO and since external stakeholders are coming into the picture, prior cyber incidents and controls which are in place to prevent incidents will be under heavy scrutiny. When an internet-based company has high quality cyber security with a great track record of preventing cyber incidents, the dollar value per share could potentially benefit from this. With the growing interest in cybersecurity, it is also in the best interest of the company to perform frequent audits and train their employees so that the company stays compliant with the government legislations.

Assuming these are the best three options available for Jashopper, I would recommend implementing solution C to impress the shareholders.

Appendices

Mitigation costs

The below table shows the mitigation costs for the solutions A, B and C

First Year Mitigation Cost (Source: Exhibit 11)	A	B	C
Set Up cost (One time)	¥300,000.00	¥2,820,000.00	¥3,320,000.00
Recurring Cost (Monthly)	¥300,000.00	¥300,000.00	¥300,000.00
Total Cost (Annual) First Year	**¥3,900,000.00**	**¥6,420,000.00**	**¥6,920,000.00**
First Annual Security Expenditure (% of Revenues)	**0.39**	**0.642**	**0.692**

Asset value calculation

The asset value of the customer server was set to 8.88 Yen based on the following calculation. The case mentions that kukaku.com had a cost of 8884.54 Yen per registered user **(200 million divided by 22511)** but Jashopper does not have that many number of users and hence we are scaling it down by **dividing the value of kukaku.com by 100**. It is also to be noted that the data of Softbank and Uji are not considered because they are internal threats and it is irrelevant to the threat statement we are assuming

Let us now calculate the asset value of Employee server. We have some benchmark value from the Morrisons case. The company was paid 170 million sterling pounds in compensation for leak of employee data by the EU court. The **170 million pounds corresponds to around 10000 employees**. To calculate the asset value, we convert 170 million pounds to Yen and do the below calculation:

(242620250 * 20)/10000 which is equal to 49240.50 Yen, we also have to add the amount of money used by the firm for damage control and with the using the Morrison's data we scale the value to 20 employees and the additional cost will amount to 28944000 Yen. Hence, we have **¥29,928,810.00** as the asset value for Employee server

ARO assumptions

Using the exhibit 7 in the case, we are using data relevant to that of Jashopper to calculate the ARO

Cybersecurity Incidents	Threat Agent	# of Incidents/3 Months	Annual Rate of Occurance (ARO)
Information Theft due to "Winny"	Outsider	1	4
CD-ROM Theft	Human	1	4
Theft of HDD	Human	2	8
Theft of Microfilm	Human	5	20
Theft of USB drive	Human	1	4
Laptop Theft	Human	1	4
PC Theft	Insider	1	4

The calculation is done as follows:

If there are 4 cyber incidents per year, the ARO percentage is (¼)*100 which is 25%. The other ARO percentages are calculated similarly

References

- https://www.bna.com/facebook-ipo-and-disclosure-of-cybersecurity-and-privacy-risks/?amp=true
- https://www.law360.com/articles/906894/5-ways-ipo-prospects-can-boost-cybersecurity-readiness
- https://www.mayerbrown.com/-/media/files/news/2018/09/sec-concerns-on-cybersecurity/files/1809rossi/fileattachment/1809rossi.pdf
- https://gettingthedealthrough.com/area/72/jurisdiction/36/cybersecurity-japan/
- https://www.gibsondunn.com/wp-content/uploads/documents/publications/WebcastSlides-IPO-and-Public-Company-Readiness-Cybersecurity-28Feb17.pdf
- https://www.teiss.co.uk/news/morrisons-data-breach-compensation/
- https://www.bbc.com/news/uk-45793598
- https://www.sec.gov/rules/interp/2018/33-10459.pdf
- https://www.osler.com/en/resources/governance/2013/corporate-review-november-en/cybersecurity-considerations-for-public-companies