JEFFORD CASE STUDY

Making Information Risk Mitigation Decisions

ISTM 635 – 603

SUBMITTED BY

SANDHEEP SRIDAR

Estimating Asset Value

The calculation of asset value for the devices of Jefford is straightforward. The primary device in question is the laptops, but the value of the data in the laptops differ based on each departments. The case describes laptops of three departments namely Salesforce, Engineering and R&D, Management and also provides the number of laptops in each department (Lacorte, p. 4). Hence, to calculate the asset value the average cost of losing data for each laptop is multiplied with the number of assets in each department. The calculation is shown below:

Asset Description	Quantity	Cost of data loss	Asset Value (AV)
Sales Force	2350	$ 500,000.00	$ 1,175,000,000.00
Enginners/R&D	650	$ 5,000,000.00	$ 3,250,000,000.00
Management	1500	$ 2,000,000.00	$ 3,000,000,000.00
Total Number of Laptops	**4500**	**$ 7,500,000.00**	**$ 7,425,000,000.00**

Estimating SLE

SLE or Single loss expectancy is the product of exposure factor and Asset Value. We are assuming the exposure factor of all the assets to be 1. The reason is because of the fact that the device is fully compromised if the encryption is broken. Furthermore, we are assuming that the exposure factor remains the same even after any kind of encryption is implemented as the case suggests that the best possible solution will be effective 97% of the time.

So, it should be noted that there is still a 3% chance of the laptop's data being compromised. The below table shows the SLE calculation for Jefford.

Asset Description	Quantity	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)
Sales Force	2350	$ 1,175,000,000.00	1	$ 1,175,000,000.00
Engineers/R&D	650	$ 3,250,000,000.00	1	$ 3,250,000,000.00
Management	1500	$ 3,000,000,000.00	1	$ 3,000,000,000.00
Total Number of Laptops	**4500**	**$ 7,425,000,000.00**		

Estimate of ARO

ARO or Annual Rate of Occurrence is the number of times the Jefford devices get affected each year. The probability of laptop theft and data loss is given in the below table:

Likelihood of Data loss AFTER laptop theft=	0.0100000
Annual Probability of Salesforce Laptop Theft=	0.0200000
Annual Probability of Engineer Laptop Theft=	0.0050000
Annual Probability of Management Laptop Theft=	0.0070000

Note: The above numbers represent probability in numbers up to 7 decimal places

These numbers will be used in calculation of the ARO as follows. The ARO for Salesforce devices will be the annual probability of theft of Salesforce devices multiplied by the likelihood of data loss after theft, The ARO for Engineering devices will be the annual probability of theft of Engineering devices multiplied by the likelihood of data loss after theft and similarly for the management laptops.

The below table shows the ARO value after performing the above calculation:

Asset Description	Quantity	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Annual Rate of Occurance (ARO)
Sales Force	2350	$ 1,175,000,000.00	1	$ 1,175,000,000.00	0.00020000
Engineers/R&D	650	$ 3,250,000,000.00	1	$ 3,250,000,000.00	0.00005000
Management	1500	$ 3,000,000,000.00	1	$ 3,000,000,000.00	0.00007000
Total Number of Laptops	**4500**	**$ 7,425,000,000.00**			

Estimate of ALE before controls

ALE or Annual Loss expectancy is the product of SLE and ARO. In the prior sections we have estimated these values for all three departments and the below table shows the ALE values before encryption is implemented:

Asset Description	Single Loss Expectancy (SLE)	Annual Rate of Occurance (ARO)	Annual Loss Expectancy (ALE)
Sales Force	$ 1,175,000,000.00	0.00020000	$ 235,000.00
Engineers/R&D	$ 3,250,000,000.00	0.00005000	$ 162,500.00
Management	$ 3,000,000,000.00	0.00007000	$ 210,000.00
Total Number of Laptops			**$ 607,500.00**

Estimate of ALE after applying controls

The case mentions that the range of solutions for encryption starts with $40 and the costliest implementation will be $140. Also, the $140 worth implementation will have and efficiency of 97%. Hence, there is a chance of the data being lost even after encryption. So, the ARO values should be recalculated again and the Exposure factor will remain the same.

For this case, we are assuming that effectiveness of the encryption decreases exponentially with cost. Also, it should be noted that most popular algorithms for encryption and decryption like RSA are based on exponential ciphers. The below table shows the ideal encryption cost, effectiveness and ineffectiveness of the encryption used.

Laptop	Encryption/Laptop	Effectiveness	Probability of breach
SalesForce	$ 90.00	90%	0.0984544
Engineer/R&D	$ 140.00	97%	0.0309242
Management	$ 135.00	97%	0.0348317

The equation used to calculate the effectiveness is

$$Effectiveness = \frac{1}{1 + EXP(cost\ of\ encryption)}$$

$$The\ probability\ of\ breach = 1 - Effectiveness$$

The below table shows the ALE values after applying the encryption controls

After Encryption			
Asset Description	**Single Loss Expectancy (SLE)**	**Annual Rate of Occurance (ARO)**	**Annual Loss Expectancy (ALE)**
Sales Force	$ 1,175,000,000.00	0.00001969	$ 23,136.78
Enginners/R&D	$ 3,250,000,000.00	0.00000155	$ 5,025.18
Management	$ 3,000,000,000.00	0.00000244	$ 7,314.65
Total Number of Laptops		**TOTAL**	**$ 35,476.61**

The below table shows the cost benefit calculation for Jefford devices

*Cost of Encryption = Number of device * total cost of control*
Benefit of Encryption = ALE before – ALE after
NRRB = Benefit of Encryption - Cost of Encryption

Cost of Encryption	Benefit of Encryption	NRRB	Recommended?
$ 211,500.00	$ 211,863.22	$ 363.22	Yes
$ 91,000.00	$ 157,474.82	$ 66,474.82	Yes
$ 202,500.00	$ 202,685.35	$ 185.35	Yes
$ 505,000.00	**$ 572,023.39**	$ 67,023.39	Yes

Recommendation: Should Mary implement encryption for the laptops?

Data is a valuable asset for any company. After analyzing the benefit of encrypting the laptops, I would recommend Mary to implement encryption for company's laptops (for all departments) with the following prices:

1. The R&D and engineering laptops have to be implemented with the highest quality of encryption available, which is $140. It is an obvious fact that Engineering and research team will have a lot of sensitive data which will be lost as the case mentions
2. Mary should invest the least on Salesforce department with $90 encryption. The solution is still viable but the reason for investing less because the cost of data theft is the lowest among all at $500,000.
3. Finally, Mary should invest $135 encryption for management laptops. The case mentions that the management laptops have strategic information and cost of data theft is the second highest with $2million. Also, we can assume that management laptops have more possibility of theft or damage because executives will be travelling with them all the time. Hence, $135 is an ideal investment for Jefford.

If Mary pitches the above recommendation with the data and cost benefit analysis, the board can be convinced and encryption solutions which will hugely benefit Jefford can be implemented

References

- Lacorte, V. L. (n.d.). Making Information Risk Mitigation Decisions.
- https://crypto.stackexchange.com/questions/35631/exponential-cipher-theory-misunderstanding

Spreadsheet:

Jefford spreadsheet google drive