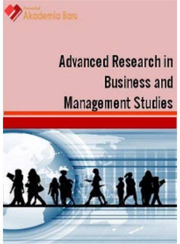
Penerbit Akademia Baru

Journal of Advanced Research in Business and Management Studies

Journal homepage: www.akademiabaru.com/arbms.html

ISSN: 2462-1935



RROI analysis in assessing risk of open source software in organization: A case study in Malaysia

Open Access

Yasmin Salim[1], Chang Tzu Enn[1], Syaza Hamzah[1], Masnita Misiran[1,*] , Hasimah Sapiri[1]

[1] Department of Mathematics and Statistics, School of Quantitative Sciences, Universiti Utara Malaysia, 06010 Kedah, Malaysia

ARTICLE INFO

Article history:
Received 28 June 2017
Received in revised form 15 August 2017
Accepted 16 August 2017
Available online 20 September 2017

Keywords:
RROI analysis, open source software, cybercrime

ABSTRACT

This paper describes the process of assessing risk for open source software in an organization. The process starts with identification of internal and external risk in an organization. Then, the potential of proactively securing organization’s system will be analyzed before the threat arises. Risk-based return on investment analysis is used to measures the effectiveness on how the organization uses the resources to proactively reducing the risk. It involve the steps of quantifying the cost of resources in one particular place to accommodate the mitigation plan. Further, the result will be compared to the cost of resources in all places in case of reactive effort. Finding shows that effort to proactively secure company from threats by using antivirus should be conducted with estimation of calculated risk-based return on investment is more than 1820%.

1. Introduction

Organization that widely uses open source software (OSS) in R&D are concerned with any security breaches in their system. Open source software are modifiable by anyone, furthermore they are able to distribute their own version of these unwanted programs without paying a licenses fees or other restrictions on the software. Such scenario allows equivalent chances for any cyber threats to penetrate into organization [33]. In consequences, the risk of theft on intellectual property (IP), the spread of all possible spyware, malware, virus and denial of service (DoS) attack, to name just a few are common in organization that adopt these OSS. Such clean up in the aftermath of these cybercrime is significantly more expensive than the crime itself [17].

As cybercrime has becoming a business where it poses the biggest threat in any organization, in which criminals considered this crime to be more profitable than drug trade, it is reported that cybercrime expenses will continue to climb sharply if no further action are taken. Since more business companies are moving online, cybercrime will damage the company performance and the national economies. Cybercrime also damages business trade, competitiveness, innovation, and global

[*] *Corresponding author.*
E-mail address: Masnita Misiran (masnita@uum.edu.my)

economic development [17]. As such, even one case of cyber-attack in organization is able to greatly affect organization.

An organization can reduce this OSS risk by identifying current internal and external risks. Internal risks refer to risk from within the organization and normally arise during normal operations of the company. Common factors for internal risks include human factors, technological factors, and physical factors. Internal risks usually happen during normal operation of the company such as stability, organizational structure, and incentives, to name just a few. Stability of a business organizations is about the ability of an organizations to finance its operations, its debt obligations and to grow more profits. Meanwhile, organizational structure is about to enhance their business operations by evaluating its workers positions, hierarchy and lines of communication. Incentives also can be one of internal risk to the organization, in particular if it is not done correctly, fairly and appropriately to the employees.

Meanwhile, external factors are events or condition that arise from outside of the organization such as the country’s economy, political legal factors and technology, to name a few. Country’s economy will definitely have an impact on the organization since it is uncontrollable. However, it is important to understand such threat and handle it during its boom or bust time. Political legal factors that involves changes in government structures or government policies will also affects business operations. Whereas for technology risk, it is important for organization to monitor technological developments in their field for their business to remain relevant [7, 10, 21, 27].

Following the strategies laid by Stoneburner *et al*. [25], there are four possible options for assessing OSS risks in organization such as the following:

a. Reducing security risk: Implementing appropriate technologies and tools (e.g. antivirus, firewall) or adopting securities policies (e.g. password, port blocking).

b. Transferring security risk: Outsourcing service provision bodies or insurance agency.

c. Avoidance of security risk: Eliminating the source of risk or asset’s exposure to the risk.

d. Acceptance of security risk: Involve the security risk as part of business operation.

In this article, we will focus on reducing security risk by analyzing the potential of proactively securing organization’s operating system before the threat arises. As proposed by the literatures, a proactive measure to secure organization from possible threats significantly reduce organization’s vulnerability. Such efforts include Khorshed *et al*. [15] and Kandias *et al*. [14] that suggested proactive threat detection model to reduce risk in cloud computing and YouTube platform respectively, while Bhatt *et al*. [4] proposed a framework to better detect threats that are multi-stage and advanced in nature. Barnum [2] not only proposed proactive counter measure to defeat threats, they also suggested a sharing of relevant cyber threat information among trusted organizations to better handle such threats. Our concern in this work is in particular on external factors of cyber-attack which likely to be a public attack that are trying to break into the organization as open source software.

We will make use of risk-based return on investment (RROI) analysis to assess advantages of using the proposed proactive security in the organization. This analysis is a popular accounting metric to compare business investment, in particular on how much the organization will get from the spent amount of money. It has widely been used in economics, such as works by Richard *et al*. [22], McNulty *et al*. [19], Kleemann [16], Satiman *et al*. [24] to name just a few; and Bashir and Christin [3]. However, to our knowledge, there are limited number of works on using this analysis to be adopted in the field of information technology, in particular in assessing the advantage/disadvantage to proactively securing OSS threat in organization. Only exceptions include work by Bojanc and Jerman-Blazic [5] that adopted this analysis to quantify risk in information security.

2. Methodology

In method selection, we are using risk-based return on investment (RROI) analysis. RROI is also known as Sharpe ratio example which is a measure of an investment's return. For this case, it measures the effectiveness on how the organization uses the resources to proactively reducing the risk by quantifying the cost of resources in one place to accommodate the mitigation plan, compared to the cost of resources in all places in case of reactive effort.

Assessing the Risks

We used RROI to measure the effectiveness on how the organization can use its resources to proactively reducing the risk posed by the aforementioned threats. The underlying idea of this proactive analysis is to quantify cost of resources in one place to accommodate the mitigation plan, as compared to considering cost of resources in all places in case of reactive effort.

3. Data

In this article, we will use the primary and secondary data.

3.1 Internal Source: Open Source Repository (OSR)

We collect data which contains number of open source software available in the organization. These OSS is grouped into different types of the category used in organization's R&D department. Table 1 shows current data of tools category on the number of OSS in the organization with approximately 7832 open source software available in the OSR running on different type of Operating System (OS).

Table 1
List of Tools Categories available in OSR

Tools Categories	Number of Tools / Category
Compiler	42
Database	4
Editor	10
General	185
Image	10
Libraries	97
Security	4
System	4
Utilities	85
Web Browser	7
Total	**448**

We consider 10 categories of OSS, namely the compiler, database, editor, general, image, libraries, security, system, utilities and web browser. The detail of these categories is presented in Table 2.

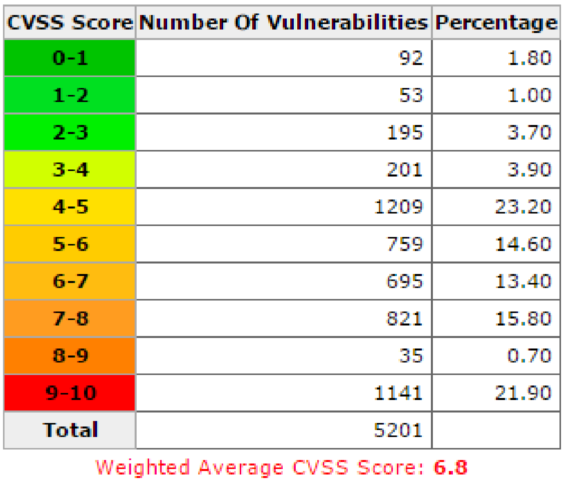
Table 2
OSS Categories

OSS Category	Function
Compiler	*Used in writing programming which transforms the source code to another computer language.*
Database	*Used to collect, organize, manage and store the Information. (e.g. MySQL-web application development)*
Editor	*Software that can easily modifiable as source code.*
General	*Has a large range of software. For example, in general, it has included pdf viewer, spreadsheet and retrieves email from remote.*
Image	*Graphical software that user can use to create and manipulate their graphics.*
Libraries	*Included libraries of general, graphics, font, programming, network library and X library. For example, the open source software of Pango library which is used for laying out and rendering of text that can use internationally.*
Security	*Has the software that will help to connect the remote computer in the quick and easy way.*
System	*A free system that public can download and use. The most common open source system is Linux.*
Utilities	*Include three categories which are general, system and network utilities. Utilities can include server software, tape achieve, documentation reader and so on.*
Web browser	*Used to browse the website. In the category of the web browser, the example given are Arora, Firefox, Thunderbird and others.*

3.2 *External Source: Common Vulnerabilities and Exposures Details*

An external source for easy use of web page is called common vulnerabilities and exposures (CVE) system. This system provides reference method for the publicly known information security vulnerabilities and exposures from national vulnerability database (NVD). Its web page compiled all related information on vulnerability. Table 3 shows number of vulnerabilities together with vulnerability range (with percentage) throughout the year 2016.

Table 3
Distribution of vulnerabilities in Year 2016



CVSS Score	Number Of Vulnerabilities	Percentage
0-1	92	1.80
1-2	53	1.00
2-3	195	3.70
3-4	201	3.90
4-5	1209	23.20
5-6	759	14.60
6-7	695	13.40
7-8	821	15.80
8-9	35	0.70
9-10	1141	21.90
Total	5201	

Weighted Average CVSS Score: **6.8**

Table 3 indicates the common vulnerability scoring system (CVSS). This scoring system is a framework for finding a solution to quantify the level of vulnerabilities in the software by standardizing their scoring system. Such system is able to help organization to strategically make informed decision in solving the vulnerabilities problem of the software.

3.3 Calculating the Risk

We make use of employee's basic salary as standard of calculation. The salary of employee in IT department is RM3500 per month. We divide this salary by approximating 20 working days in a month will give the cost per day as RM175.

To assess the uncertainty of the cyber-attack, we use Bayesian approaches which gives $P(Y \leq y)$, as in Equation 1.

$$P(Y \leq y) = \int P(Y \leq y|\theta)dH(\theta), \tag{1}$$

where *H* is the level of cyber-attack.

With this test, we are indicating that the computer system is having cyber-attack because of the open source software that they are using. Let *X* be 1 and 0 according test on OSS which given positive or negative response of being attacked.

Table 4
Situation of system under attack

	Situation of Organization's system is under attack
0	Under low risk
1	Under medium risk
2	Seriously high risk
3	Critical risk

Table 4 assumes that the company will be facing situation of being under attack. The percentage of the CVSS is used to calculate Ɵ, the risk of cyber-attack for OSS.

Table 5
Score of CVSS

CVSS score	**Percentage**	**Under Attack**
0.1 - 3.9	0.104	0
4.0 - 6.9	0.512	1
7.0 – 8.9	0.165	2
9.0 – 10.0	0.219	3

Table 5 shows the percentage score of the CVSS which is aligned with Table 4.
We illustrates the calculation as follows:

Table 5
Percentage of CVSS score

CVSS Score	Value
$\mathbf{0.1\ \mathit{to}\ 3.9}$	$\frac{1.80+1.00+3.70+3.9}{100}=0.10$
$\mathbf{4.0\ \mathit{to}\ 6.9}$	$\frac{23.2+14.60+13.40}{100}=0.512$
$\mathbf{7.0\ \mathit{to}\ 8.9}$	$\frac{15.8+0.7}{100}=0.165$
$\mathbf{9.0\ \mathit{to}\ 10.0}$	$\frac{21.9}{100}=0.219$

Further, we test the positive response of cyber-attack, as illustrated in Table 6. Let the percentage of denial of service be 0 which is the system is under lower risk, code execution 1, overflow 2 and bypass something & gain privileges 3, which poses critical risk towards the system.

Table 6
Vulnerability Trends Over Time for Open office (from CVE details)

Year	# of Vulnerabilities	Denial of Service	Code Execution	Overflow	Bypass something	Gain Privileges
2002	1					1
2004	3		2	1		
2005	2	1	1	1	1	
2006	5	1	2	3		
2007	6	1	5	3		
2008	2	1	1	1		1
Total	19	4	11	9	1	2
% Of All		21.1	57.9	47.4	5.3	10.5

From Table 6, we can formulate the following conditional probabilities:

$$P\ (X=1|\theta=3)=\frac{10.5+5.3}{100}=0.158$$
$$P\ (X=1|\theta=2)=\frac{47.4}{100}=0.474$$
$$P\ (X=1|\theta=1)=\frac{57.9}{100}=0.579$$
$$P\ (X=1|\theta=0)=\frac{21.1}{100}=0.211$$

By combining all probabilities of positive cyber-attack of OSS, P(X=1) = P(X=1|Ө =3)P(Ө =3) + P(X=1| Ө =2)P(Ө =2) + P(X=0| Ө =1) +

P(X=0|Ө=0)P(Ө =0)

= 0.158×0.219 + 0.474×0.165 + 0.579×0.512 + 0.211×0.104

= 0.4312.

Now, we calculate posterior distribution by using Bayes' theorem,

$$f(\theta|x) = [L(\theta)f(\theta)]/f(x) \quad (2)$$

where f is a general express distribution of the cyber-attack.

Critical risk will affect the system by the open source software

P (Ө =3|X=1) = [P (X=1|Ө =3) P (Ө =3)]/ P (X=1)
= (0.158 x 0.219)/0.4312
= 0.0802

Seriously high risk will affect the system by the open source software

P (Ө =2|X=1) = [P (X=1| Ө =2) P (Ө =2)]/ P (X=1)
= (0.474 x 0.165)/0.4312
= 0.1814

Medium risk will affect the system by the open source software

P (Ө =1|X=1) = [P (X=1| Ө =1) P (Ө =1)]/ P (X=1)
= (0.579 x 0.512)/0.4312
= 0.6875

Low risk will affect the system by the open source software

P (Ө =0|X=1) = [P (X=0| Ө =2) P (Ө =0)]/ P (X=1)
= (0.211 x 0.104)/0.4312
= 0.0509

Table 7
Expected loss from cyber-attack towards open source software per year

Risk	Probability of cyber attack	Day to recover	Expected loss per attack outcome (RM)	Cyber-attack per year (RM)
critical	0.0802	10	26250	327306.7332
high	0.1814	8	21000	115766.2624
moderate	0.6875	6	15750	22909.09091
low	0.0509	3	7875	154715.1277
Total				620697.2142

By making use of the previous calculation, we approximate the expected incurred loss of organization in Table 7. The expected loss is calculated by using the standard employee's salary as mentioned in previous subsection. We consider human resource to be 15 employees which is in line with current number of employees in the IT department.

Table 8 shows the protection against malware attack available online by AV-TEST. AV-TEST suggested that average protection against 0-day malware attacks inclusive of web and e-mail threats in organization takes up to 98% effort through Real-World Testing of 162 samples.

The risk return on investment (in %) is calculated as follows

RROI = [Total expected loss of cyber-attack per year – (Total price of antivirus per
year × capability of protection against malware attack)]/ Total price of
antivirus per year

$$\text{RROI} = \frac{RM620{,}697.2142 - (RM32{,}345 \times 0.98)}{RM32{,}345} = 18.21$$

Table 8
RROI-Risk Return on Investment

No. of laptop/computer of the company	250
Price of antivirus per year (RM)-refer website of Mc Afee for small business	129.38
Total price of antivirus Mc Afee per year (RM)	32345
Protection against malware attack (average)	0.98
RROI-Risk Return on Investment (%)	1820.989687
RROI (RM)	**588,352.2142**

The findings showed that by using proactive solution in organization, i.e. adopting antivirus software to protect the cyber-attack from OSS threats will give strong countermeasure of the risk return on investment (RROI) of approximately 18.21 or 1,821%. Such estimation also suggests the prevention of risk avoidance totaling of RM588,352.21 in monetary value, where the amount of cyber-attack per year totaling to RM620,697.21 to be subtracted from the price of antivirus per year (RM32,345.00).

4. Conclusion

In this study we provide a simple model of RROI for quantitative risk analysis of proactive securing the organization in any possible threats. Based on the findings, organization should take proactive action to securing their organization from possible threats with the effort of installing antivirus throughout their organization. Such proactive way needs to be done if the company would like to use open sources software in their company. As open sources do not use a licenses, possible risks will always be there even though the company is able to create their own internal program. By using antivirus as proactive counter measure, prevention to possible risks is expected to save approximately RM 588,352.21 in monetary value, with RROI's percentage at 1820% efficient. Organization should also use proactive action by prior scanning softwares using CVE. If the software falls in dangerous level, the software should be removed.

Among initial steps to prevent the risk include establishing staff training program to maintain user awareness of the cyber risk, filter out unauthorized access and malicious content to protect organization's networks against external and internal attack, and consistently monitor and test security controls.

References

[1] AV-TEST - The Independent IT-Security Institute. The best antivirus software for Windows Home User (2016) Retrieved from: https://www.av-test.org/en/antivirus/home-windows/windows-7/august-2016/mcafee-internet-security-2016-163164/

[2] Barnum, Sean. "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)." *MITRE Corporation* 11 (2012): 1-22.

[3] Bashir, M., and Nicolas Christin. "Three case studies in quantitative information risk analysis." In *Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop*, pp. 77-86. 2008.

[4] Bhatt, Parth, Edgar Toshiro Yano, and Per Gustavsson. "Towards a framework to detect multi-stage advanced persistent threats attacks." In *Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on*, pp. 390-395. IEEE, 2014..

[5] Bojanc, Rok, and Borka Jerman-Blažič. "A quantitative model for information-security risk management." *Engineering Management Journal* 25, no. 2 (2013): 25-37.

[6] Berg, Heinz-Peter. "Risk management: procedures, methods and experiences." *Risk Management* 1, no. 17 (2010): 79-95.

[7] Bernard, C. (2013). Risks in business: Internal and external pressures. Retrieved from https://home.kpmg.com/xx/en/home/insights/2013/07/business-risks-internal-external-pressures.html.
Cambridge dictionary- http://dictionary.cambridge.org/dictionary/english/

[8] CVE Details: The ultimate security vulnerability datasource. (2016). Retrieved from: http://www.cvedetails.com/cvss-score-charts.php

[9] Darryll, H. (n.a). *Evaluation of Value-At-Risk Models Using Historical Data.* Retrieved from:
https://www.newyorkfed.org/medialibrary/media/research/epr/96v02n1/9604hend.pdf

[10] Epstein, Marc J., and Adriana Rejc. *The reporting of organizational risks for internal and external decision making*. CMA Canada, 2006.

[11] Intel Security McAfee. Essential Security for Businesses-McAfee Endpoint Protection Essential for SMB. Retrieved from:
http://www.shopmcafee.com/store?Action=pd&Locale=en_US&SiteID=mfesmb&categoryID=66300400&productID=306911700

[12] Intel Security Mcafee (2014). Net Losses: Estimating the Global Cost of Cybercrime, economic impact of cybercrime II, Center for Strategic and International Studies. Retrieved from: https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[13] Isom, C. J., and David R. Jarczyk. "Innovation in Small Businesses: Drivers of Change and Value." *Ceteris Inc* (2009).

[14] Kandias, Miltiadis, Vasilis Stavrou, Nick Bozovic, and Dimitris Gritzalis. "Proactive insider threat detection through social media: The YouTube case." In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pp. 261-266. ACM, 2013.

[15] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." *Future Generation computer systems* 28, no. 6 (2012): 833-851.

[16] Kleemann, Linda, Awudu Abdulai, and Mareike Buss. "Certification and access to export markets: Adoption and return on investment of organic-certified pineapple farming in Ghana." *World Development* 64 (2014): 79-92.

[17] Losses, Net. "Estimating the global cost of cybercrime." *McAfee, Centre for Strategic & International Studies* (2014)..

[18] McNeil, Alexander J., Rüdiger Frey, and Paul Embrechts. *Quantitative risk management: Concepts, techniques and tools*. Princeton university press, 2015.

[19] McNulty, Yvonne, Helen De Cieri, and Kate Hutchings. "Expatriate return on investment in the Asia Pacific: An empirical study of individual ROI versus corporate ROI." *Journal of World Business* 48, no. 2 (2013): 209-221.

[20] Mell, Peter, Karen Scarfone, and Sasha Romanosky. "Common vulnerability scoring system." *IEEE Security & Privacy* 4, no. 6 (2006).

[21] Ng, S. C. Y., and M. Bakhtiarib. "Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis."

[22] Richard, Patrick, Kristina West, and Leighton Ku. "The return on investment of a Medicaid tobacco cessation program in Massachusetts." *PLoS One* 7, no. 1 (2012): e29665.

[23] Sano, Fumikazu, Takeshi Okamoto, Idris Winarno, Yoshikazu Hata, and Yoshiteru Ishida. "A Cyber Attack-Resilient Server Using Hybrid Virtualization." *Procedia Computer Science* 96 (2016): 1627-1636.

[24] Satiman, Luqman Hakim, Nur Naha Abu Mansor, and Nadiatulhuda Zulkifli. "Return on Investment (ROI) training evaluation in Malaysian SMEs: factors influencing the adoption process." *Development and learning in Organizations* 29, no. 2 (2015): 18-21.

[25] Stoneburner, Gary, Alice Y. Goguen, and Alexis Feringa. "Sp 800-30. risk management guide for information technology systems." (2002).

[26] Stoner, James. A.F. and Freeman.E.R., 1989. Management, Prentice Hall of India, New Delhi.

[27] Thiab, A. S., and A. S. Shibghatullah. "Hypervisor Security Issues in Cloud Computing: The Need to Mitigate the Risks." *Advanced Research in Computing and Applications* 1: 1-5.

[28] The Open Source Definition. URL: http://www.opensource.org/docs/definition.php. accessed on October 14, 2016.

[29] Perens. B, (2008). *The Open Sources Definition*. MTFSTU

[30] Rider, G., Milkovich, S., Stool, D., Wiseman, T., Doran, C. & Chen, X. (2010). *Quantitative Risk Analysis.* Retrieved from http://www.tandfonline.com/doi/abs/10.1076/1566- 0974(200006)7:2;1-R;FT115

[31] N. A. (2016). *Return on Investment ROI Explained : Definition, Meaning, Example Calculation.* Business Encyclopedia. Retrieved from https://www.business-case- analysis.com/return-on-investment.html

[32] Openoffice: Vulnerability Statistics (2016, November 30) Retrieved from: https://www.cvedetails.com/product/2603/Openoffice-Openoffice.html?vendor_id=1510

[33] Vadalasetty, Sreenivasa R. "Security concerns in using open source software for enterprise requirements." *SANS Institute* (2003).

[34] West, Joel, and Scott Gallagher. "Challenges of open innovation: the paradox of firm investment in open-source software." *R&d Management* 36, no. 3 (2006): 319-331.

[35] Williams, L.(2004) Generic Risks Product-Specific Risks. Retrieved from: http://agle.csc.ncsu.edu/SEMaterials/RiskManagement.pdf