2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Quantifying the Return of Security Investments for Technology Startups

Mohamed Noordin Yusuff Marican*[1]*, ***Siti Hajar Othman[1], ***Ali Selamat***[1, 2, 3, 4]***
Shukor Abd Razak[5]

[1]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.
[2]Malaysia-Japan Institute of Technology, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.
[3]MaGICX-Media and Game Innovation Centre of Excellence, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.
[4]Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove, Czech Republic.
[5]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia.
*Corresponding Author.

Received 05/06/2023, Revised 01/09/2023, Accepted 03/09/2023, Published Online First 25/12/2023, Published 1/7/2024

Abstract

Technology startups are critical to the advancement of digital initiatives in many countries undergoing smart nation agenda. Technology startups are thus vendors and suppliers of services to large organizations such as the government sector, multi-national corporations and financial institutions. As such, startups are fast becoming attack vectors for malicious perpetrators to gain entry via backdoors to large organizations. However, startups remain prudent in their cyber security spending as their north star is revenue generation by delivering their services and minimum viable product (MVP) to their customers. This study proposes an enhanced Return on Security Investment (ROSI) which helps technology startups calculate the return on security investment and justify their budget of cyber security spending. Though there are existing models to calculate the return of investments allocated to cyber security expenditure, they are rather complex and do not give management clarity in terms of the monetary value for cyber security spending. Furthermore, the existing models do not cater to the dynamics and nuances of technology startups. The enhanced model also provides technology startups the ability to appropriately adjust their cyber security investments based on the calculations of the Minimum (Min) and Maximum (Max) ROSI values. The proposed and enhanced ROSI model has been validated by 5 cyber security experts who agreed on the importance and necessity of the model to be applied to technology startups. The results of the case study on a FinTech startup enable the calculation of the Min and Max ROSI to justify the return on security investments and provide the startup with the ability to adjust the cyber security spending accordingly.

Keywords: Cyber Security Maturity Level, Cyber Security Quantification, Return of Security Investment, ROSI, Technology Startup.

Introduction

In this day and age, digitalization is no longer an option. In the current digital era, no organization is safe from the proliferation of cyber-attacks which occur on a daily basis. Cyber criminals are relentless

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

in finding new ways to exploit security vulnerabilities in organizations at a global scale[1]. Whether you are a large multinational conglomerate, financial institution, government agency, small and medium enterprises (SMEs) or even a technology startup, the threat of a cyber-attack is not the matter of "if" it will occur but rather "when" it will occur. That is why it is important for organizations, big or small, being "cyber-ready" or equipped with the right resources to protect and defend against cyber threats. According to Singapore Business Review, Singapore, a small sovereign state in Southeast Asia, has detected 1,817,635 cyber threats in Q2 2022 alone which is an increase of 17.6% from Q1.

Cyber-attacks, whether they are in the form of data breaches, ransomware, denial of service or exploitation of vulnerabilities, can cost organizations a lot of money and in the case of SMEs such as technology startups, they may even end up closing up shop. SMEs are the same as startups in the form of scale and size[2]. They typically do not have many employees unlike large multinationals and are especially prudent in their spending due to limited financial capability. They play a critical role in the economic and social stability of the country[3]. In the case of technology startups where the main focus is on developing innovative products for the end consumers, the budget is typically allocated for product development, and not on enhancing cyber security capabilities, which thus makes technology startups even more susceptible to cyber-attacks by malicious perpetrators[4]. Founders in technology startups don't normally comprehend the concepts of cyber security. Generally, in startups, cyber security is viewed as an IT problem but in actual fact, it has to be acknowledged as a business risk. When the organization suffers a data breach due to a cyber-attack, it has an adverse impact on the company reputation, customers' churn and investors' confidence. The attack may hamper the startup's ability to scale, attract new customer base or investments from venture capitalists.

Since startups have limited financial resources to invest in cyber security, they do not have the necessary capabilities to protect their business from cyber-attacks. This is why hackers have shifted their attention to attack smaller organizations like startups instead of putting their efforts on large conglomerates[5]. Unbeknownst to end users, technology startups are vendors to numerous large organizations ranging from the government sector, financial institutions, multinational companies and even other SMEs or technology startups. As such, these technology startups have access to confidential and proprietary information such as employees' and customers' personal data, intellectual property, sensitive project details and these startups may even have a network connection linking them to large organizations, especially in cases involving business-to-business (B2B) customers.

In order for technology startups to build trust in the business ecosystem, it is critical for them to be equipped with adequate cyber security measures to combat the inevitable threat of cyber-attacks[5]. Hence, there is an essential need for startups to have the ability to make informed decisions on the investments that should be allocated to cyber security and quantifying the return of investments which they have made.

With an increased number of cyber threats, regulatory scrutiny and the introduction of new cyber security and data protection policies and standards, organizations are placed under pressure to ensure compliance[5] and technology startups are no exception. Security should not be perceived as a profit-making catalyst for the organization, but instead, as a mechanism to reduce loss or exposure[6]. Thus, investments in cyber security are not only viewed as critical but play a strategic role for the organization to scale[7]. Calculating the return of security investment involves a combination of both qualitative and quantitative approaches which is no easy task, however the results can enable technology startups to make strategic decisions when investing in cyber security. If the return of security investment generates a positive value that would mean the investments made to build or enhance the security capabilities are justified. A negative return would ultimately mean that the investment is not worth it, and hence would cost more than the exposure value. Basically, it will not make economic sense to implement a security solution which costs more than the impact of the risk.

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

This research proposes a modified Return of Security Investment (ROSI) model catered for technology startups to make informed decisions to justify the need to invest on cyber security measures. The rest of this research is divided into four sections. The literature review section analyses the relevant studies pertaining to cyber quantification, including its limitations. The next section proposes an enhanced ROSI framework which enables technology startups to calculate ROSI and justify their spending on cyber security. The following section consists of the results on a case study to validate the modified ROSI model in a technology startup and finally the last section concludes the research with some future directions.

Analysis of Relevant Studies

To assist with the literature review, a survey was conducted to understand the commonly-used cyber quantification models that are used by industry cyber security practitioners. The survey respondents consist of mid to senior level cyber security professionals from technology startups, SMEs, consulting firms and multi-national conglomerates. The cyber security practitioners range from C-level executives such as Chief Technology Officers (CTOs), Chief Information Security Officers (CISOs), Heads of Information Security, Managers and Assistant Managers in Information Security and Cyber Security Consultants.

As shown in Table 1 below, 54% of the respondents are not using any cyber quantification model to calculate the return of security investments. 23% leverage on Bayesian Networks, 8% use Monte Carlo Simulation while 23% of the respondents use other non-specified models. Based on search results when queried on cyber quantification models, the Factor Analysis of Information Risk (FAIR) and Return of Security Investment (ROSI) frequently appear in journal articles including supporting journal papers. Based on the results shown in Table 1, there is no standardized cyber quantification model which is used by industry practitioners in technology startups to calculate the return of security investments. A high number of respondents who do not use any cyber quantification model found that the existing models are too complex.

Table 1. Survey for Cyber Quantification Model

Which Cyber Quantification model you typically leverage on?	
Monte Carlo Simulation	8%
Bayesian Networks	23%
Others (please specify)	15%
Too Complex – I don't use any!	54%

In this study, the Monte Carlo Simulation, Bayesian Networks, FAIR and ROSI are analysed to determine their appropriateness for use in technology startups. Ultimately, the key objective is to come up with an appropriate model which is able to analyse the return of security investments in technology startups so that budgets for security investments can be allocated and justified accordingly. The analysis of the selected models is as follows:

a) FAIR: The FAIR or Factor Analysis of Information Risk model was developed by Jack Freund and Jack Jones[8]. Classified by[9] as another variation of the Monte Carlo simulation, FAIR is used to analyse risk and quantify loss events. The loss events are security incidents which could vary from website defacements, data breaches or distributed denial of service attacks. The loss events are further broken down into loss frequency and divided into six categories; Productivity Loss, Response Costs, Replacement Costs, Competitive Advantage, Fines/Judgement and Reputational damage[10]. The losses are then quantified based on a range of estimates. The Annual Loss Expectancy (ALE) is later calculated where a graph is plotted to give an estimation of the loss pertaining to the threat event.

Analysis of the loss is subjective which is dependent on the Loss Event Frequency (LEF) and Loss Magnitude (LM). The LEF and LM values can easily be misinterpreted. Furthermore, there isn't a remediation cost to determine whether there are safeguards to prevent future losses, and if the safeguards are justifiable to provide a positive return of security investments.

In a case study to quantify the risk for a vulnerability pertaining to the Government-to-Citizen (G2C) service launched in Estonia, the FAIR model had been used to calculate the loss in dollar amount over a period of time[11]. It was noted during the expert validation of this model that the importance of

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

budgeting was highlighted several times when the cyber security practitioners raised concerns that even with a large budget, cyber security gaps still exist. As such, there is a need to calculate the minimum and maximum remediation costs so that the budget can be adjusted accordingly to address the key risks.

b) Monte Carlo Simulation: The Monte Carlo Simulation provides a number of probable scenarios where data is input to produce an output in order to generate a range of likely losses. In an example of a ransomware attack using the approach by Hubbard & Siersen, the probability of the risk event happening in Company X is 70% and there could be a likely loss of $100,000 to $500,000. Using Monte Carlo Simulation, the Loss Exceedance Tolerance and Expected Losses are computed. The Loss Exceedance Tolerance is able to justify whether the expected losses have exceeded the acceptable loss tolerance.

The Monte Carlo Simulation can be used to calculate the expected inherent and residual loss and the data can be used to make decisions on security investments. However, there can be more than one event affecting the organization and this model did not take into consideration of key controls where in the lack thereof could be a consequence of another loss event. Basically, in the case of a technology startup, not analysing the key controls can prevent the quantification of loss pertaining to the threat if the key control is lacking in the organization. Calculating the loss without determining the remediation costs prevents the organisation's ability to allocate an appropriate budget to mitigate any security risk events.

c) Bayesian Networks: Bayesian Networks work on the basis of probability which consists of variables that place reliance upon each other. Bayesian networks have been used not only in cyber security but in other areas of study and industry sectors such as banking and manufacturing. Bayesian network is another model which can be used to quantify cyber risks that can influence the justification of security investments. The Bayesian model uses equations to calculate the probability of a security incident through various probable scenarios (e.g., exploitation of vulnerability, data breach, probability of data breach based on discovery via penetration test, etc). The final calculation generates the resultant values to show the probability of the following scenarios, as an example:

- Probability of a vulnerability
- Probability of a major data breach
- Probability of a major data breach if a vulnerability is exploited
- Probability of a major data breach after the vulnerability is discovered during a penetration test
- Probability of major data breach after a penetration test which failed to detect the vulnerability which can be exploited

In the study by Wolthuis et al., the Bayesian Networks model to quantify the probability of a risk event[12]. Though the model was able to quantify risks probability with current datasets, there are several limitations such as the following:

- A significant amount of effort is required to develop a model for one threat.
- Information required is difficult to obtain as the retrieval involves several areas in the organisation.
- It is challenging to translate the information collected into probability.
- The model does not have provisions to analyse budgets for security investments.

In conclusion, Bayesian networks can be used to calculate the probability of the occurrence of security events, and hence quantify the potential losses and remediation costs. However, the rate at which the incident could happen is based on estimation and will produce a challenge to come up with a more accurate value.

d) Return of Security Investment (ROSI): The Return of Security Investment (ROSI) is a commonly used method to calculate and justify the return of security investments. ROSI works on a much reasonable level of probability pertaining to the annual rate of incident occurrences or ARO, and hence justifies the need to purchase the remediation measures in order to

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

mitigate the risks. ROSI is expressed as a percentage based on the following formula[13]:

$$\text{ROSI (\%)} = \frac{[(\text{ALE} \times \text{\% of Risk Mitigation}) - \text{Cost of Solution}]}{\text{Cost of Solution}} \quad (1)$$

Where;

ALE refers to the Annual Loss Expectancy representing the total monetary loss for the year due to security incidents which is calculated by the Annual Rate of Occurrence (ARO) multiplied by the Single Loss Expectancy (SLE). ARO is the number of security incidents which occur in the year while SLE is the amount of money which is lost due to a single incident which has occurred. The limitation of the ROSI model is that the ARO is subjective. Four security incidents can happen in the previous year, but it does not mean exactly four will occur the following year. Furthermore, the cost of the solution can be broken down into resources such as headcount as it may not be necessarily related to purchasing hardware or software solutions in order to remediate the risk exposure.

The ROSI model had been utilised in several literature with various case studies[14, 15]. Whilst the model has provisions to calculate the return of security investment, it only provides with the maximum returns based on the ARO. This limits the organisation's ability to quantify the appropriate budget for the remediation of security risks.

The models which have been analyzed in this section do serve a purpose in terms of quantifying cyber security risks and losses. However, further steps and a more concrete version of the model would need to be considered to accurately calculate the return of security investment. Table 2 has provided a comparison of the relevant cyber quantification models. While ROSI seems to be the most applicable cyber quantification model compared with FAIR, Monte Carlo Simulation and Bayesian Networks, it has key deficiencies in terms of producing accurate results as the ARO can be subjective. Furthermore, the lack of a mathematical model to calculate the range of ROSI prevents the organization from coming up with an appropriate budget to remediate security risks.

Technology startups are known to be lean and thrive on innovating products and deliver services at scale[16]. As such, it is important to develop an efficient model to calculate the return of security investment in a simplified manner so that startups are able to allocate appropriate budget to justify their spending on cyber security.

Table 2. Comparison of the relevant Cyber Quantification Models

Model / Features	FAIR	Monte Carlo Simulation	Bayesian Networks	ROSI
Organisation Type	All	All	All	All
Type of Industry	All	All	All	All
Purpose	The quantification of cyber risk to justify cyber security investments	Loss quantification to justify cyber security investments	The quantification of cyber risk to justify cyber security investments	The calculation of the Return of Security Investment
Applicability of model for use in Technology Startups	Medium	Low	Low	High
Relevance of model for use in cyber security	Analysis and quantify cyber risk	Analysis of probabilities on cyber security scenarios	Assess cyber security dependencies, risks and impact	Able to calculate the return of cyber security investments
Mathematical formula to calculate the range of ROSI	No	No	No	No
Key Deficiency	Remediation costs is lacking in	Key controls are not analysed which may	The rate of incident occurrence is	The annual rate of occurrence is

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

	determining the returns of security investment	result in inaccurate loss quantification	estimated which may be subjective and not produce accurate results	subjective and may not produce accurate results

Proposed Return of Security Investment Model for Technology Startups

The proposed model to calculate the return of security investment utilizes the current ROSI model but with a modified variable which is the Annual Rate of Occurrence (ARO). In the existing ROSI model, the ARO which is the measure of the number of incidents occurring on an annual basis is determined by approximation through interviewing the stakeholders (e.g., information security practitioners). This approximation is based on the stakeholder's experiences which are determined by historical security incidents. Small companies such as technology startups are busy with other key priorities and do not emphasise the importance of cyber security which allow hackers to focus their attention on them[17]. As such, they are susceptible with the proliferation of cyber-attacks due to the lack of adequate cyber security protection compared to the larger organizations which have the resources to defend against cyber threats[17, 18].

Hence, it is imperative that technology startups are able to right-size their budget allocation on cyber security measures to not only protect themselves against cyber threats, but also receive positive returns on their cyber security investments. In order to achieve optimum value in the budget allocation, startups need to accurately determine the ARO. However, the limitation of this approximation is that the value is based on probability which may differ from the number of incidents that could potentially occur. Furthermore, this judgement on the probability is dependent on the experience of the security practitioner and whether the practitioner has been with the organisation for a reasonable period of time where he could provide an informed approximation based on historical data. With the modified ARO variable in the enhanced ROSI to determine the Minimum and Maximum ARO, the ALE and ROSI are also modified allowing practitioners to have an overview on the minimum and maximum return of security investments. This helps technology startups with an accurate picture to adjust the budget accordingly in order to procure cyber security solutions to remediate the security risk. Fig .1 below illustrates the flowchart of the Modified Return of Security Investments (ROSI) with detailed explanations from sections 3.1 to 3.6 to calculate the Min and Max ROSI expressed in percentages.

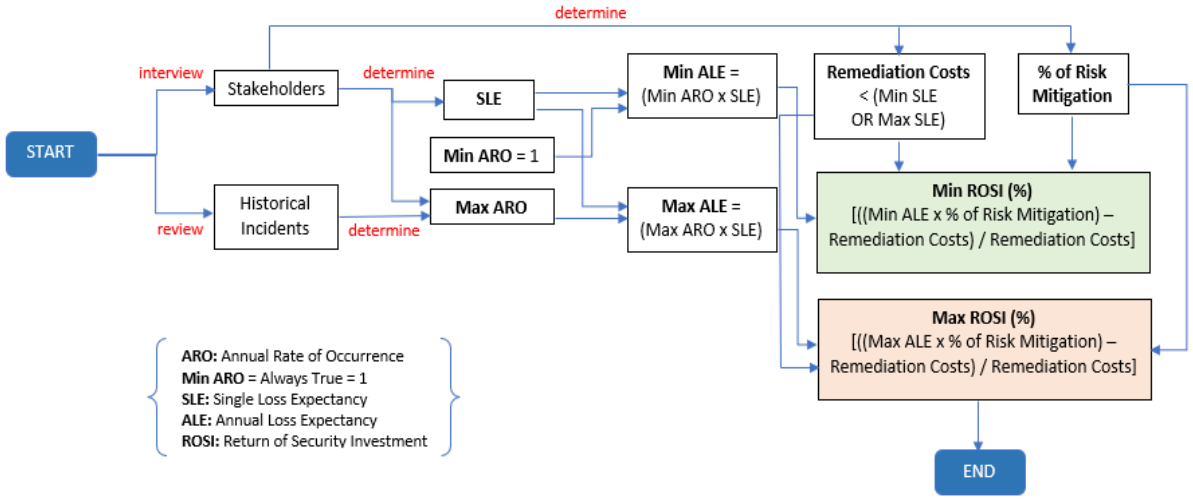

Figure 1. Flowchart for Modified ROSI

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Minimum and Maximum Annual Rate of Occurrence

The ARO metric is divided into 2 categories which are the Minimum (Min) and Maximum (Max) ARO. The Min ARO is the proposed variable introduced in this equation and given a value of 1 (one). This means that the ARO is always true and thus, the minimum number of incidents that is expected for the year is at least 1. The occurrence of security incidents is a matter of "when" rather than "if". As such, it is only prudent to indicate at least one occurrence of the incident for the year due to the lack or absence of the key control. The Max ARO is still determined via approximation with the security practitioner and the value is based on the practitioner's experience and historical incidents. This equates to $1 \leq n \leq x$ where n is the number of probable incidents and x is the maximum number of incidents that could occur in the year. As such;

$$\text{Min ARO} = 1 \quad (2)$$

$$\text{Max ARO} = n \quad (3)$$

Single Loss Expectancy (SLE)

The Single Loss Expectancy or SLE metric refers to the expected amount of monetary loss based on a single security incident. Though the SLE is based on professional judgement, it gives management an estimate when a loss is realized due to a security incident. Security incidents can result to financial penalties, reputational loss due to media publication, decreased revenue and lost in employees' productivity. The losses can be the result of both direct and indirect costs. Direct costs are tangible in nature such as financial penalties imposed by the regulators or revenue loss suffered by the company due to the security incident. Indirect costs are less tangible in nature which still has a negative impact on the business such as reputational loss and employees' productivity.

Annual Loss Expectancy (ALE)

This metric calculates the amount of expected monetary loss for the year based on the risk impact due to the lack of a specific key control in the organisation. The Annual Loss Expectancy or ALE is thus divided into Min ALE and Max ALE which corresponds to the Min and Max ARO respectively:

$$\text{Min ALE} = \text{SLE} \times 1 \quad (4)$$

$$\text{Max ALE} = \text{SLE} \times \text{Max ARO (n)} \quad (5)$$

Remediation Cost

The remediation cost is another variable in the ROSI equation that provides the monetary amount to implement a safeguard or fix a failed control to prevent future occurrence of security incidents. This can involve purchasing of security solutions, implementation costs, hiring of security staff or outsourced contractors. Remediation costs are typically direct costs which can be obtained by the stakeholder or security practitioner. It is however important to note that the Remediation Cost should never be more than the Min or Max SLE which equates to:

$$\text{Remediation Cost} < \text{SLE (min or max)} \quad (6)$$

If the remediation cost is more than the Min or Max SLE, it will not make business sense to implement the safeguards as the return of security investment will be a negative value. It will hence be better to either accept or terminate the risk. Terminating the risk means eliminating the risk either by removing or altering the risky process.

Percentage of Risk Mitigation

The risk mitigation variable is expressed in percentage. Risk mitigation defines the percentage of risk which can be mitigated when the remediation or safeguard is implemented on the key control. This risk mitigation can help to ensure that the confidentiality, integrity, availability and accountability of the asset (e.g., servers, data) are maintained. The percentage of risk mitigation is determined by the security practitioner based on professional judgement. Typically, most security practitioners have the experience and knowledge to provide a reasonable approximation on the percentage of risk mitigation.

Modified Return of Security Investment (ROSI)

The return of security investment is broken up into Min ROSI and Max ROSI. The Min ROSI utilizes the variables Min ARO and Min SLE while the Max ROSI uses Max ARO and Max SLE as the variables. Having Min and Max ROSI gives management a range based on the minimum and maximum rate of

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

incident occurrences. The Min and Max ROSI are both expressed in percentages as per eqs. (7-8) below respectively:

$$\text{Min ROSI (\%)} = \frac{[(\text{Min ALE} \times \text{\% of Risk Mitigation}) - \text{Remediation Costs}]}{\text{Remediation Costs}} \quad (7)$$

$$\frac{[(\text{Max ALE} \times \text{\% of Risk Mitigation}) - \text{Remediation Costs}]}{\text{Remediation Costs}} \quad (8)$$

Comparison of Modified ROSI with Relevant Models

The key element in the mathematical formula of the Modified ROSI is the Minimum and Maximum ARO or the Annual Rate of Occurrence. Since cyber-attacks can happen unknowingly, it is practical to indicate ARO = 1 where there will be at least one occurrence of incident for the year due to the absence of a key control. The maximum ARO would still provide provisions to anticipate the number of incidents that will happen when comparing with historical data. With Min and Max ARO, the mathematical formula in this section produces the Min and Max ALE, and ultimately the Min and Max ROSI. Using the above equations, this would also enable organisations to adjust the remediation costs upwards or downwards to facilitate the positive returns of security investment. This is especially important for technology startups which are typically prudent in their spending and thus, would like to ensure that they get the best returns of investments on their cyber security spend.

As per Table 2 which highlighted the selected Cyber Quantification models in this study based on existing literature and survey results, they do provide the quantification of losses and return of investments, however one key element which fails is the ability to produce the range of ROSI based on the minimum number of expected incidents. By having the Min and Max values in the Modified ROSI mathematical formula, smaller startups with smaller budgets can adjust the allocation of security investments accordingly while the larger startups can either invest more or less based on the Min and Max ROSI which have been calculated. All the four cyber quantification models which have been identified in this study lack this ability, and thus enable the Modified ROSI to produce an accurate cyber security budget and the true value on the return of security investments.

The modified ROSI has its own limitation when startups need to quantify losses related to cyber security attacks as the quantification of losses is subjective since the ARO varies. Cyber security spend is nonetheless a necessity in any organisation due to evolving cyber threats across the globe. Hence, startups, as prudent as they are, should instead utilise the modified ROSI to ensure they do not overspend on cyber security but instead right-size their budget accordingly to adequately protect their organisation.

Results and Discussion

The proposed enhanced Return of Security Investment (ROSI) model has been validated by 5 experts who are cyber security practitioners including conducting a case study on a technology startup. This strategy of validation supports the contribution of the proposed ROSI for technology startups.

Expert Validation Feedback

A walkthrough was conducted with 5 cyber security experts from various industries in order to assess the proposed mathematical eqs. (1-7) which have been derived to calculate the return of security investments. The key objective of the experts is to validate the equations which have been formulated to calculate the return of security investments and assess their suitability for use in technology startups.

The profile of the experts is detailed in Table 2 below. In order to gain insights from subject matter experts with varied numbers of years of experience, experts with more than 5 to 20 years of experience in cyber security were chosen and they must be previously or currently responsible for leading the

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

cyber security function in their respective organizations. Experts from different industry sectors were also selected to obtain varying insights from different industries. Expert 1 worked in a technology startup and government organization in his previous experience and is currently working in the healthcare sector. The expert experience provides a blend of both startup and traditional cyber security practices. Expert 2 is the owner of his own consulting startup providing cyber security advisory services for clients ranging from technology startups, government organizations and multi-national corporations. The insights from Experts 1 and 2 are valuable as they provide varied perspectives on the application of cyber security practices in both established corporations and technology startups. Experts 3 to 5 are heading their respective cyber security functions in technology startups for the Digital Banking, Telecommunications and FinTech industries. Experts 3 to 5 have the latest and updated knowledge on cyber security practices in technology startups.

Table 3. Profile of Experts

S/N	Role	Type of Startup
1	Head of Security	Healthcare
2	Head of Information Security	Cybersecurity
3	Deputy Chief Technology Officer	Digital Bank
4	Lead, Cyber Security Operations	Telecommunications
5	Chief Information Officer	FinTech

To validate the appropriateness of the calculations in the ROSI model, the eqs. (2-8) were presented and explained in detailed to the 5 experts. The questions shown in Table 3 below have been derived to validate the proposed ROSI model.

All the 5 experts have chosen "Agree" which thus validates the entire proposed and enhanced ROSI model which can be utilised in technology startups. During the validation sessions with the respective experts, all of them have acknowledged the importance and necessity of this model which allows startups to not only justify the return of their security investments but also provide the ability to adjust their security budget in the most optimal way.

Table 4. Experts Response

S/N	Questions	Expert Response
1	The ARO is appropriate to be determined by the stakeholders and similar incidents which occurred in the past.	~~Disagree~~ / ~~Not Sure~~ / Agree
2	It is reasonable to compute the minimum ARO = 1 to represent the least number of incidents which could occur in the absence of a key control.	~~Disagree~~ / ~~Not Sure~~ / Agree
3	The calculations to compute Min SLE and Max SLE are appropriate based on the Min ARO and Max ARO.	~~Disagree~~ / ~~Not Sure~~ / Agree
4	The remediation costs must always be less than the Min SLE and Max SLE.	~~Disagree~~ / ~~Not Sure~~ / Agree
5	Based on the computed variables, the ROSI formula has been appropriately enhanced to compute the Min ROSI and Max ROSI for management to justify and right size cyber security investments for technology startups.	~~Disagree~~ / ~~Not Sure~~ / Agree

Case Study Validation

A case study was conducted on a FinTech startup to validate the appropriateness and suitability of the proposed enhanced ROSI model. This startup has been chosen as it falls under the category of a "technology startup" and fits into the target segment of this study. For the case study, it was assumed that the risk and control assessment has been conducted in which the risks due to the lack of key control have been identified and the risk treatment plan has been suggested in order to remediate the risk.

As an example, for the case study, one of the key controls for endpoint security is to implement a Data Loss Prevention (DLP) tool in all endpoints to prevent intentional or unintentional leakage of data.

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Data security is critical to protect users' privacy in organisations[19]. During the interview with the Chief Technology Officer (CTO) in the FinTech startup, none of the users have installed the DLP. Hence, there is a risk of accidental data leakage due to the lack of DLP implementation. As part of the risk treatment plan, the startup should speed up the process to procure and ensure the DLP tool is installed on users' endpoints in the immediate future to prevent the risk of data leakage.

Applying the ROSI model to the above-mentioned risk and via conducting interviews with the CTO, the calculations are determined as follows for the Min and Max ARO:

Min ARO = 1 9

Max ARO = 4 10

Based on eq. 10 above, the CTO has acknowledged that there have been at least 4 incidents in the past which involve the leakage of sensitive data, though they are all purely accidental after the investigation was conducted. Thus, Max ARO = 4. The Min ARO is equal to 1 as instead of a re-occurrence of 4 incidents which may or may not occur during the year, there is still a high possibility of at least 1 incident which could potentially be materialized during the year. Thus, Min ARO = 1.

On the Single Loss Expectancy or SLE, the CTO indicated that an incident of data leakage could result in costs involving a financial penalty by the regulator, hiring of forensic investigators and the potential loss of customers. This would cost the company at least $200,000 (SLE = 200,000) in the event of data leakage. Thus, the Min and Max ALE are calculated as follows:

Min ALE = 200,000 x 1 = 200,000 11

Max ALE = 200,000 x 4 = 800,000 12

In order to mitigate the risks of data leakage, the FinTech startup would need to procure the DLP solution which would cost around $100,000 (Remediation Cost = 100,000). Since DLP is well known as an effective tool to prevent data leakage, the CTO is certain that the percentage of risk mitigation can be estimated at 95% (% of Risk Mitigation = 95%). Applying the Min and Max ROSI formula, the calculation is determined as follows:

$$\text{Min ROSI (\%)} = \frac{[(200{,}000 \times 0.95) - 100{,}000]}{100{,}000} \quad 13$$

Min ROSI = 90%

$$\text{Max ROSI (\%)} = \frac{[(800{,}000 \times 0.95) - 100{,}000]}{100{,}000} \quad 14$$

Max ROSI = 660%

Based on the Min and Max ROSI calculations above, procuring the DLP solution which cost $100,000 to prevent the risk data leakage produces a return of security investment ranging from 90% to 660%. This proves that procuring the remediation measure (i.e., DLP) generates a reasonable return of security investment and hence, the investment is justified. With the value of Min and Max ROSI above, the CTO in the FinTech startup could also adjust and negotiate the cost of remediation accordingly with the DLP vendor before procuring the solution in order to ensure that the return of security investment is positive.

Conclusion

It goes without saying that technology startups are playing a vital role in assisting the economy to thrive forward in this digital area of innovation and smart nation building. Having the right cyber security resources and measures is critical not only for the survival of startups against malicious perpetrators but also for large organizations that are connected and working hand in hand with the startups. When startups are hit by a data breach, it impacts investors and customer's confidence and may result to churn and loss of future investments. Technology startups hence need to dig into their funds in order to allocate investments on cyber security in order to protect themselves against cyber threats. It is known to date that there is no one model to calculate the return of security investments which can be agreed upon by security practitioners[20]. Admittedly, there isn't a one-

size-fits-all model when it comes to calculating and justifying the returns of security investments.
The proposed and enhanced ROSI model has provided much clearer and more accurate calculations to adjust and justify the remediation costs and calculate the return of security investments. The results from both the expert validations and case studies of the FinTech startup have provided a reasonable level of assurance on the appropriateness of the proposed model to be used in technology startups.

Future studies can be conducted by applying this model across different industry segments for technology startups including large organizations to determine whether they are able to determine the return of security investments in a shortened timeframe and get a more accurate picture on the remediation costs and ultimately measure the return on investments on their cybersecurity spend. The application of this model can be further compared with the application of other cyber quantification models in the same environment to determine its benefits from the cost, manpower requirements, and completion timeframe and accuracy perspective.

Authors' Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at University of Teknologi Malaysia.

Authors' Contribution Statement

This work has been carried out in collaboration between all authors. M. N. Y. M. developed the research idea under the supervision of S.H.O., A. S. and S. A. R. All authors read and approved the final manuscript.

References

1. Abdullah SA, Al Ashoor AA. IPv6 Security Issues: A Systematic Review Following PRISMA Guidelines. Baghdad Sci J. 2022; 19(6): 1430-1444. https://doi.org/10.21123/bsj.2022.7312
2. Zuszsanna C. Startup: Hype or Tendency. J Org Culture Commun. Confl. 2020; 24(3): 1-9. https://www.abacademies.org/articles/Startup-hype-or-tendency-1939-4691-24-3-144.pdf
3. Ozkan BY, Spruit M. Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects. ArXiv. 2020; 1-8. https://doi.org/10.48550/arXiv.2007.01751
4. Mitrofan AL, Cruceru EV, Barbu A. Determining the Main Causes that lead to Cyber Security Risks in SMEs. Bus Excell Manag. 2020; 10(4): 38-48. https://doi.org/10.24818/beman/2020.10.4-03
5. Ozkan BY, Spruit M. Adaptable Security Maturity Assessment and Standardization for Digital SMEs. J Compute. Inf Syst. 2022; 63(4): 1-23. https://doi.org/10.1080/08874417.2022.2119442
6. Sonnenrich W, Albanese J, Stout B. Return on Security Investment (ROSI) – A Practical Quantitative Model. J Res Pract Inf Tech. 2006; 38(1): 46-56. https://doi.org/10.5220/0002580202390252
7. Niedzela LM, Albanese J, Stout B. Categories of Approaches for IT Security Investment Decisions: A Systematic Literature Review. Wirtschaftsinformatik 2022 Proceedings; Jan 17. Nuremberg, Germany. Atlanta, GA: AIS eLibrary; 2022. p. 1-7. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1270&context=wi2022
8. Puangsri P. Quantified Return on Information Security Investment – A Model for Cost-Benefit Analysis. Netherlands: Delft University of Technology; 2019. https://silo.tips/download/a-model-for-cost-benefit-analysis
9. Hubbard DW, Seiersen R. How to Measure Anything in Cybersecurity Risk. 2nd ed. Hoboken: Wiley; 2023. 280 p. https://doi.org/ 10.1002/9781119162315
10. Freund J, Jones J. Measuring and Managing Information Risk: A FAIR Approach. 1st ed. Oxford: Butterworh-Heinemann; 2014. 408 p. https://doi.org/10.1016/C2013-0-09966-5
11. Dreyling III R, Jackson E, Pappel I. Cyber Security Risk Analysis for a Virtual Assistant G2C Digital

Service using FAIR Model. 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG); September 2021. Quito, Ecuador: IEEE; 2021. p. 33-40. https://doi.org/10.1109/ICEDEG52154.2021.9530938

12. Wolthuis R, Jongsma H-J, Phillipson F, Langenkamp P. A Framework for Quantifying Cyber Security Risks. Cyber Security Peer. 2021; 4(4): 302-316. https://hstalks.com/article/6342/a-framework-for-quantifying-cyber-security-risks/
13. Podesva L, Koch M. Comparison of the Most Important Models of Investments in Cyber and Information Security. Trend Econ Manag. 2022; 39(1): 25-34. https://doi.org/10.13164/trends.2022.39.25
14. Paresh R, Timo H. A Novel Model for Cybersecurity Economics and Analysis. 17th IEE International Conference on Computer and Information Technology; September 2017. Helsinki, Finland: IEEE; 2017. p. 274-279. https://doi.org/10.1109/CIT.2017.65
15. Yaqoob T, Arshad A, Abbas H, Amjad M-F, Shafqat, N. Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations. Future Gener. Comput. Syst. 2018; 95: 754-763. DOI: https://doi.org/10.1016/j.future.2018.12.033
16. Rasmussen ES, Tanev S. The Emergence of the Lean Global Start-up as a New Type of Firm. Technol Innov Manag. 2015; 5(11): 12-19. http://doi.org/10.22215/timreview/941
17. Pawar S, Palivela H. LCCI: A Framework for Least Cybersecurity Controls to be implemented for Small and Medium Enterprises (SMEs). Int J Inform Manage. 2022; 2(1): 1-13. http://dx.doi.org/10.1016/j.jjimei.2022.100080
18. Chandna V, Tiwari P. Cybersecurity and the New Firm: Surviving Online Threats. J Business Strategy. 2021; 44(1): 3-12. https://doi.org/10.1108/JBS-08-2021-0146
19. Al Mayyahi MA, Seno SAH. A Security and Privacy Aware Computing Approach on Data Sharing in Cloud Environment. Baghdad Sci J. 2022; 19(6): 1572-1580. https://doi.org/10.21123/bsj.2022.7077
20. Onwubiko C, Onwubiko A. Cyber KPI for Return on Security Investment. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment; June 2019. Oxford, UK. Piscataway, NJ: IEEE; 2019. p. 1-8. https://doi.org/10.1109/CyberSA.2019.8899375

2024, 21(7): 2449-2461
https://doi.org/10.21123/bsj.2023.9077
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

تحديد عائد الاستثمارات الأمنية للشركات التقنية الناشئة

محمد نوردين يوسف ماريكان [1]، سيتي حجر عثمان [2]، علي سلامت[1,2,3,4] ، شكور عبد الرازق [5]

[1]كلية الحوسبة، جامعة تكنولوجيا ماليزيا، جوهور بهرو، ماليزيا.
[2]معهد ماليزيا اليابان للتكنولوجيا، جامعة تكنولوجيا ماليزيا، جوهور بهرو، ماليزيا.
[3]مركز تميز ميديا وابتكار الألعاب MaGICX، جامعة تكنولوجيا ماليزيا، جوهور بهرو، ماليزيا.
[4]كلية علوم المعلومات والإدارة، جامعة هراديتش كرالوفي، هراديتش كرالوفي، جمهورية التشيك.
[5]كلية علوم الحاسوب والمعلومات، جامعة سلطان زين العابدين، كوالا ترغكانو، ماليزيا.

الخلاصة

تعتبر الشركات الناشئة في مجال التكنولوجيا بالغة الأهمية في النهوض بالمبادرات الرقمية في العديد من البلدان التي تخضع لأجندة الدولة الذكية. وبالتالي ، فإن الشركات الناشئة في مجال التكنولوجيا هي بائعون وموردون للخدمات للمنظمات الكبيرة مثل القطاع الحكومي والشركات متعددة الجنسيات والمؤسسات المالية. على هذا النحو ، أصبحت الشركات الناشئة سريعًا نواقل هجوم للجناة الخبثاء للدخول عبر الأبواب الخلفية إلى المؤسسات الكبيرة. ومع ذلك ، لا تزال الشركات الناشئة حكيمة في إنفاقها على الأمن السيبراني لأن نجمها الشمالي هو توليد الإيرادات من خلال تقديم خدماتها والحد الأدنى من المنتجات القابلة للتطبيق (MVP) لعملائها. تقترح هذه الدراسة عائدًا معززًا على الاستثمار الأمني (ROSI) والذي يساعد الشركات الناشئة في مجال التكنولوجيا على حساب العائد على الاستثمار الأمني وتبرير ميزانيتها للإنفاق على الأمن السيبراني على الرغم من وجود نماذج حالية لحساب عائد الاستثمارات المخصصة لنفقات الأمن السيبراني ، إلا أنها معقدة نوعًا ما ولا تعطي وضوحًا للإدارة من حيث القيمة النقدية للإنفاق على الأمن السيبراني. علاوة على ذلك ، لا تلبي النماذج الحالية ديناميكيات وفروق الشركات الناشئة في مجال التكنولوجيا. يوفر النموذج المحسّن أيضًا للشركات الناشئة في مجال التكنولوجيا القدرة على تعديل استثماراتها في مجال الأمن السيبراني بشكل مناسب بناءً على حسابات قيم الحد الأدنى (الأدنى) والحد الأقصى (الأقصى) لمؤشر .ROSI تم التحقق من صحة نموذج ROSI المقترح والمحسّن من قبل 5 من خبراء الأمن السيبراني الذين اتفقوا على أهمية وضرورة النموذج الذي سيتم تطبيقه على الشركات الناشئة في مجال التكنولوجيا. تتيح نتائج دراسة الحالة الخاصة بشركة FinTech الناشئة حساب Min و Max ROSI لتبرير العائد على الاستثمارات الأمنية وتزويد الشركة الناشئة بالقدرة على ضبط الإنفاق على الأمن السيبراني وفقًا لذلك.

الكلمات المفتاحية: مستوى نضج الأمن السيبراني، تقييس الأمن السيبراني، العائد على الاستثمار الأمني، الشركات التقنية الناشئة.