Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. *International Journal of Critical Infrastructures*, *13*(2-3), 152-167. https://doi.org/10.1504/IJCIS.2017.088235

Towards Effective Cybersecurity Resource Allocation: The Monte Carlo Predictive Modelling Approach

Abstract: Organisations invest in technical and procedural capabilities to ensure the confidentiality, integrity and availability of information assets and sustain business continuity at all times. However, given growing productive assets and limited protective security budgets, there is a need for deliberate evaluation of information security investment. Optimal resource allocation to security is often affected by intrinsically uncertain variables and associated factors like technical, economical and psychological; therefore, security expenditure is a crucial resource allocation decision. In spite of that, security managers and business owners are often incentivised by different drivers on whether to allocate optimal resources to cyber-specific security protective assets or other business productive assets. Hence, there is a disparity of opinion in resource allocation decisions. We explored how Monte Carlo predictive simulation model can be used within the context of Information Technology to reduce these disparities. Using a conceptual enterprise as a case study and verifiable historical cost of security breaches as parametric values, our model shows why using conventional risk assessment approach as budgeting process can result in significant over/under allocation of resources for cyber capabilities. Our model can serve as a benchmark for policy and decision support to aid stakeholders in optimising resource allocation for cyber security investments.

Keywords: Information Security, risk assessment, Resource allocation, Monte-Carlo simulation, Security investment decision.

1 Introduction

There are a lot of fundamental issues associated with risk evaluation, reporting and mitigation costs in IT security domain. The problem of cyber security risks management in corporate organisations is non-trivial, hence, constructing tools that truly satisfy risk measurement theory is difficult and not readily available [1]. Information security is fundamentally concerned with the confidentiality, integrity and availability of information assets at all times. In order to defend against threats to information assets, organisations invest in countermeasures, however, as the number of assets to be protected grows and IT budgets are constrained, there is a need for deliberate evaluation of information security investments [3]. Cyber security is one of the biggest challenges facing businesses in recent time. Economic loss due to cyber-attack is on the increase and many businesses have been obliterated due to loss of intellectual assets to cyber criminals. This figure is set to grow exponentially, according to the study conducted in [21] which enunciated that by 2020, losses from cyber-attack may hit the $20 Trillion mark. In a different report [26], studies conducted to quantify the actual and potential value of losses as a result of successful system breaches is put in the region of $500 million and $5 billion per year in the United States alone. Hence, the importance of risk management cannot be overemphasised. As firms' vulnerability to cyber-attacks increases, so is the need for further investment in cybersecurity enhancement measures. Security managers can effectively reduce the potential and probability of loss to cyber rogues by reinforcing firms' cyber capabilities. [22].

What constitutes Information Security risk, is relative to organisation risk acceptance level. However, in all cases, security managers' priority is to mitigate organisational risk exposure that could undermine the confidentiality, integrity and availability of mission-critical systems. Apart from huge financial losses, a security breach can lead to sanctions from industry regulators, negative corporate image, and loss of confidence in clients and customers. A classic example is the case of TalkTalk, a UK communication giant that was hacked in 2015. Personal details of nearly 157,000 TalkTalk customers were accessed through a rudimentary SQL Injection attack on the company website. More than 15, 000 personal account numbers and sort code were also stolen. The impact of cyber-attack is reported [27, 28] to have cost the company £42m, loss of over 100,000 customers and a fine of £400,000 for the data breach by the Information Commission Office (ICO). The ICO claimed that hacks could have been prevented if TalkTalk had implemented basic cyber security measures to safeguard its customers' data.

This work explores how Monte-Carlo simulation model can be used for effective cyber security resource allocation. It investigates how to make a business case for resource allocation decisions within a business enterprise/SMBs. Monte Carlo simulations have been extensively used by risk analysts in various fields of study to make future risk estimations [6]. A simulation approach to managing and visualising uncertainties in cyber-security context allows different variables to be applied to different risk scenarios, for optimal resource allocation to mitigate manage those risks. Monte-Carlo simulation can perform quantitative risk analysis by assigning a probability distribution to uncertain parameters; and through random sampling of the distribution, it is possible to determine all potential outcomes under those uncertainties [7].

The structure of the rest of this paper is as follows: Section 2 covers the literature review of related work. We present risk management overview in section 3. The background description of our predictive modelling approach is covered in section 4. Model assumptions, scenario and methodology are covered in section 5. We present results and key findings in section 6. Conclusion and future work implications are covered section 7.

2 Related Work

There are several works [9, 10, 11, 12], that evaluates the budgetary allocation problems of information security investments, in an attempt to justify optimum security investment decisions. The work in [25] showed how system vulnerability can be reduced through security patches. A game-theoretic model was developed to study the strategic interaction between a vendor and a firm in balancing the costs and benefits of patch management. The approach presented by [13] is based on expected utility value of investment in order to determine the optimal investment amount. The approach suggests that the level of investment for asset protection depends on the vulnerability of the asset and associated potential losses. The work further assumes that with increase information security investment, the probability of security breach decreases but the marginal improvement on security also decreases with higher investment. Hence, risk-averse management may maximise the expected utility of a budget to determine the maximum amount to invest, which should not exceed the potential loss of breach. The approach presented [14], uses the term 'Return on Security Investment' (ROSI), which is similar to the traditional accounting figure. The approach incorporates one-time costs and benefits of information security while it discards running costs and benefits as well as non-financial security measures. In order to support investment decisions. ROSI is calculated as:

ROSI = ((risk exposure x risk mitigation)-solution costs)/ (solution costs). Where: risk exposure=ALE X ARO

ALE denotes annual loss exposure while ARO denotes the annual rate of occurrence.

In a work presented by [15], information security investment decision is based on a balanced scorecard performance measuring system. This method, in its original context, evaluates organisation business performance from the angle of financial, customer, internal process and innovation. The authors extended and applied balanced scorecard method in the context of information technology to support management decisions. The approach uses goal measurement to establish investment needs. Goal importance e.g. server downtime reduction is weighted relative to other goals in order to set goal fulfilment minimum average degree. If an investment's average degree is considered to be above the threshold, then it is deemed economically viable. This approach considers all financial and non-financial mitigation measures.

There are other research efforts that also propose Monte Carlo simulation for information security. For instance, [18] Presents Monte Carlo simulation method for evaluating and communicating security investment benefits and to understand technology choices in a financial manner. In [33], the authors describe probabilistic risk assessment to ICT systems, through scenario-based estimation of agent attack plan and risk impact. Then applies Monte Carlo for detailed simulation of threat agents' behaviour to support assessment through statistical evaluation of risk. Similarly, [34] introduces Haruspex to simulate adaptive agents. The tool utilises Monte Carlo method to support evidence-based risk assessment and management, in furtherance of justifying appropriate countermeasures. The work in [35] presents a different approach to information security assessment based on analytic hierarchy process (AHP) and Monte Carlo simulation. In particular, the approach applies weight elements to the confidentiality, integrity and availability of information assets in order to improve the accuracy of results. The approach presented in [36] addresses uncertainty elements in security risk assessment and visualisation. It combines system level process through risk analysis and probabilistic survivability assessment (RAPSA) and expert estimation through Monte Carlo, in order to quantify information risks as financial variables.

However, with respect to the related publications, our work use the Monte Carlo simulation approach to optimise resource allocation for security investment in a different perspective. The work discussed in this paper is based on a predictive modelling approach and offers a different dimension to information security resource allocation problems. We applied Monte-Carlo simulation in the context of information technology to a single block optimal resource allocation at an organisational level. However, the way IT divisions prioritise budgets to different security capabilities is not included in this work.

3 Risk Management Overview

Information security risks are generally described under the broad categorization of disaster or abuse. The top priority of Chief Information Officers (CIO) and management are to ensure continual functionality of IT resources at critical levels of operations. Risk management can be described as a systematic and logical approach to identifying, treating, analysing and monitoring risks in any process. Managers benefit from risk management strategies because it has a direct bearing on how available resources are put to best use. Risk management is practised in both private and public sectors; including health care, government establishments, insurance, finance and investments. However, in the context of Information Security, risk management is about the protection of information assets. Information Security Risk Management is defined [29] as the protection of information assets from a wide range of threats in order to ensure business continuity, manage business risk and maximise return on investment. Risk management within the context of an organisation involves the implementation of appropriate controls to mitigate, share, transfer, insure, accept and continually manage risks as set out in the ISO/IEC 27001:2013 Standard [31]. The ISO/IEC2700 series of standards define best practices, baseline requirements and controls for Information Security Management Systems (ISMS), under the confidentiality, integrity and availability (CIA) triad. In addition, given that threat climate changes all the time, it is essential that the effectiveness of security controls be periodically reappraised by the organisation. This is an important element of risk management cycle [30]. There are various reasons why an organisation may require some measures of security control against potential threats; these could stem from internal factors like corporate regulations and organisational policies or mandatory external influences like the data protection acts or compliance requirements of industry regulators. Whatever the driver, it is apparent that risk management will involve some mitigation control investments and resource allocation decisions.

However, Information Security professionals often do not quantify and communicate risks effectively in order to attract the right level of resource allocation. Again, organisations may struggle to present a measure of accurate cost benefits of information security activities, primarily because, security investment results in loss prevention rather than profit margins [2]. That is why business executives often opt for compliant security, whereby, baseline requirements of standards like the ISO2700, NIST etc. are implemented, then businesses operate under the assumption that compliance equates security. Whereas, this is often not the case because baseline controls may be enough for industry regulators and business executives but often fail to result in holistic protection [32]. The costs associated with risk management range from personnel to hardware and software outgoings. Therefore, information security expenditure is a crucial resource allocation decision, yet little is known about the budgeting process used to ensure optimal investment in information security capabilities [4], or at best, the budgeting process is generally beclouded with ambiguities.

Traditionally, organisations use risk assessment model to determine the optimal allocation of resources to cyber capabilities. This approach is a flavour of risk-based regulation whereby firms determine their security investment based on risk assessment, potential losses and investment profile [23]. An organisation's budgetary decision is then based on its threat tolerance and its score from the risk scoring matrix. Risk scoring matrix is calculated on the assumption that an event will happen given a probability of occurrence and impact or severity of security breaches. Information security budget is then allocated based on the resultant estimated risk score. The risk scoring formula is given as:

$$\text{Risk} = \text{Probability (P)} \times \text{Impact (I)}$$

The value of (P) and (I) for a given asset is assigned based on expert opinion, statistic from reports, corporate level assessment or record from past events and the resultant single value represents the risk score for that particular asset. To suggest that the risk impact to information assets are subjective probability estimates is rather ambiguous and deterministic. In practice, it is difficult to apply this calculation to real world problems, in order to optimise resource allocation decisions. This approach raises the question of reliability [5], as risk predictions are misrepresented for effective mitigation. Information security risk and management is transitory; hence, the actual impact of risky events might not be a true reflection of the current deterministic estimation.

4 Background Description of our Predictive Modelling Approach

4.1 Different Approaches to Resource Allocation Decision Processes

When risk analysis is based on the traditional risk matrix approach, security assessors extrapolate that under certain assumptions, certain events would be true; while completely discarding the possibility of least significant and extreme events as part of that extrapolation. For organisations that base its threat tolerance on information security risk assessment, trying to guess the odd under so many uncertainties can only lead to erroneous results. The difficulty of this approach is further emphasised in [24], where it is stated that effective allocation of resources under the circumstance of uncertain risk and severity of breach

cost is very hard. In order to explain how uncertainty affects security breach costs and resource allocation decision to mitigate those risks, we present a high-level and low-level conceptual enterprise scenario for a bank in figure 1 and figure 2 respectively.

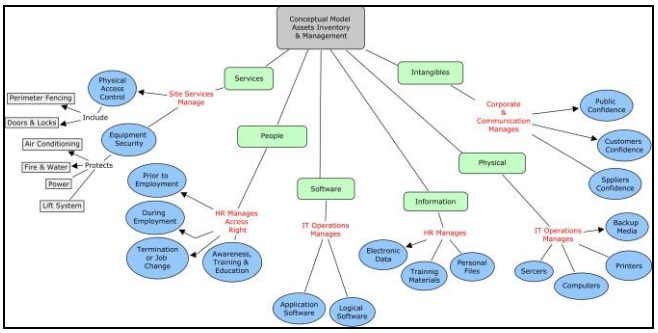

Figure 1: High-level conceptual model diagram

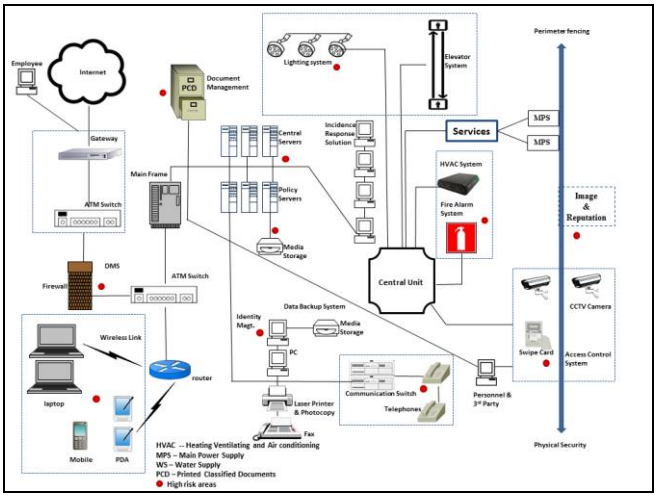

Figure 2: Low-level conceptual model diagram showing key asset points

We assume that the bank only has 5 high-risk asset points that need to be safeguarded from security threats at all times. Also, stakeholders' resource allocation decision is based on the severity of breach to those assets and how it may impact banking operation. For illustrative purposes, we consider DDoS Mitigation System, Personnel and third-party contractors, Data Backup and Recovery System, Incident Response Solution, and Antivirus Software as the key asset.

4.1.1 Deterministic Estimation of Security Breach Costs

This approach is based on the use of conventional risk assessment model to determine appropriate resource allocation. Deterministic point estimation is associated with random variability like a game of chance. In a roll of a die, probabilistically, there is a 1/6 chance that a certain number would come up, and it would have an interpretation given long-term frequency. Risk/vulnerability output based on five scale levels of very low, low, medium, high and very high also have the same element of chance. See table 1 for a description of likelihood and severity of risk, especially in terms of financial impact. Likelihood of risk is ranked on the scale of 1 to 5, where 1 is rare or very low and 5 is frequent or very high.

Likelihood	Description	Frequency of Occurrences
1	An incident is expected to occur in exceptional circumstances, e.g. once in 10 years	Rare/Very Low
2	An incident may occur at some point, e.g. once in 3 years	Possible/Low
3	An incident will occasionally recur, e.g. once in a year	Probable/Medium
4	An incident will occur in most circumstances, e.g. once every 4 months	Certain/High
5	An incident is certain to occur in most circumstances, e.g. once every month	Frequent/Very High
Severity	**Description**	**Example of Business Impact**
1	None: no disruption of service	Financial loss < £1000
2	Minor	Financial loss < £10, 000
5	Moderate	Financial loss < £100, 000
10	Significant	Financial loss < £1, 000 000
15	High	Financial loss > £1, 000 000

Table 1: Risk likelihood and severity description

Similarly, table 2 shows the risk scoring matrix by taking into account the likelihood and severity value of each risk. Risk scoring is carried out by applying a simple multiplication process whereby the likelihood of risk is multiplied by the severity of that risk occurring. After scoring each risk, risk rating is then applied by choosing the most appropriate definition under likelihood and the most appropriate definition under severity, then the numbers are

looked up in the risk matrix table and matched to obtain the risk rating. After the risk analysis phase, given an organisation risk threshold and the risk score number, the budget is allocated for countermeasures to mitigate risks in that context.

The idea of risk assessment is to evaluate scenarios of security incidents and take proactive measure before it happens. Consider one of our scenario high-risk assets; a dedicated DDoS Mitigation System (DMS) that can deter DDoS attacks. How effective the DMS is to mitigate volumetric attacks may be uncertain but it is unlikely that enterprise operations and vital computing resources will be subjected to complex layer 7 attacks, in order to ascertain if the defence mechanism is worthy of investment. Rather, it is more likely that we use historical data to assist with resource allocation decisions, but in the absence of data, we can use estimations. A risk analyst may make a statement that the probability of a successful attack without mitigation (the DMS) is 3, and the cost impact in terms of human and financial resources needed to recover from the attack is ($53,477).

Risk Rating Table – Likelihood x Severity						
Severity → / Likelihood ↓		None	Minor	Moderate	Significant	High
		1	2	5	10	15
Frequent	5	5	10	25	50	75
Certain	4	4	8	20	40	60
Probable	3	3	6	15	30	45
Possible	2	2	4	10	20	30
Rare	1	1	2	5	10	15

Table 2: Risk rating table

However, when deterministic point estimate is used to score risk and model uncertainties; what that actually mean is that based on the subjective estimates for each asset point, the total breach cost without security investment for all tangible and intangible assets in the enterprise, will always be the sum of breach costs to each asset (as shown in table 3). If it is certain that an expert's deterministic estimate is 100% reliable, then potential cost of a security breach should be fine, hence resource allocation to mitigate those risks should correctly reflect the assessment. In reality, security breach to some asset will cost less with insignificant impact while some may result in colossal losses with catastrophic consequences. Therefore, resource allocation under uncertain risk-based assessment is unlikely to match risk mitigation efforts.

4.1.2 Probabilistic Estimation of Security Breach Costs.

In order to address the huge amount of uncertainties associated with deterministic approach, especially in view of increasing information assets; we can consider probabilistic estimation approach. Through, Monte-Carlo simulations, we can determine the probabilistic cost of breach for each asset in a given scenario. The Monte Carlo simulation works by sampling lots of scenarios from a probability distribution instead of static point estimates. Probabilistic estimation assigns minimum and maximum cost boundaries for each security breach. The combined cost of all security breaches is then calculated as the total minimum and maximum cost of a security breach for each asset in order to project total resource allocation for the enterprise. In that case, it is possible to establish absolute bounds for allocated resources to the entire enterprise.

Monte Carlo may not be able to tell with certainty the exact cost of a breach, but it can describe the probability of cost associated with security breaches, to aid resource allocation. In comparison to the deterministic approach, the probabilistic estimate is also based on random variables, however, each estimate follows a particular distribution, independent and unaffected by other variables.

Average annual cost of security breach in magnitude of $K/year		
Assets	**Security Incidents**	**C = Cost of breach**
DMS	DDoS Attack	53,477
Personnel & 3rd Party	Malicious Insider	40,403
Recovery System	Data Loss	39,905
Incidence Response	Cyber Espionage	69,026
Anti-Virus Software	Malicious Code Infection	31,572
	Total	234,383

Table 3: Expert estimation of security breach costs

Consider the deterministic cost of breach for the DMS as described in the previous sub-section. Under probabilistic estimation approach, we can use a smearing out parameter to suggest that in place of a fixed quantity like £53,477, we could include the minimum value in of $30,000 and the maximum value of $65,000 in a distribution, as shown in table 4. Essentially, we replace a fixed value with a probability distribution, which is a true representation of the state in the real world. Hence, the fixed quantity is now our most likely value, but it is not the only possible value in the distribution. The key to Monte Carlo simulation is that each variable is assigned a random value, and the total value is calculated thousands of times during the simulation. It, therefore, allows us to understand the risk that expectations may not match reality, hence, appropriate precautions can be taken [8].

Assets	Security Incidents	Unit cost of security breach without risk mitigation investments (in magnitude of $K/year)		
		C_{min} = minimum	**C_{ml} = most likely**	**C_{max} = maximum**
DDoS Mitigation System	Dos/DDoS Attack	30,000	53,477	65,000
Personnel and third party contractors	Fraud/Malicious Insider	20,000	40,403	50,000
Data Backup and Recovery System	Data loss/Stolen Devices	25,000	39,905	45,000
Incident Response Solution	Cyber Espionage	35,000	69,026	75,000
Antivirus Software	Malicious Code Infection	15,000	31,572	37,000
Total		123,000	234,383	272,000

Table 4: Model simulation parameters

It is difficult to compute values for multiple scenarios without some form of simulation, especially if we have to factor in multiple assets and security breach costs, as part of the budgetary allocation process.

5 Methodology

There are two basic assumptions for this model:

- Key information asset points are determined by an organisation CIO and the security team.
- Minimum and maximum values of security breach costs are subject to expert elicitation, based on experience and previous security breach events.

The work described in this paper use some security breach cost parametric values obtained from verifiable information security breach reports. Model parameters are taken from the Ponemon Institute 2015 cost of security breach report [16], and Kaspersky Lab IT security risks special report series [17]. The study in [16] covered data breach cost and impact of 350 organisations around the globe. The study use activity-based costing (ABC) for data breach calculation which takes into account; direct cost, indirect cost and opportunity cost. It also takes into account a range of expenditure associated with organisation data breach detection, containment, response and remediation. The study in [17] covers corporate IT security risks survey of more than 5500 companies in 26 countries around the world. It covers IT threats and the cost of recovery when a security breach occurs. Values taken from both studies serve as input parameters for our simulation model as shown in table 4. However, limitations of the costing methodology outlined in the studies are not validated nor described in this work.

We identify uncertain deterministic security breach costs in our model and convert them into a range of values using a triangle distribution, as shown in figure 3. For each breach cost estimate, given an asset, fixed values are replaced with a probability distribution. Triangular distribution used in this model is one of the most used probability distributions to elicit expert opinion, especially in the case of limited or absence of historical data. It defines uncertain breach cost values as a minimum (C_{min}), most-likely (C_{ml}) and maximum (C_{max}) range of values, for each asset in the model calculations.

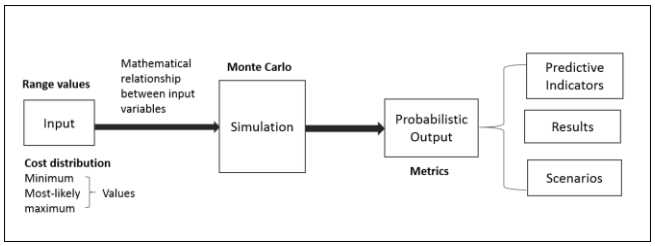

Figure 3: Schema of the MC predictive model

This approach follows the model implemented in [18], whereby the (C_{min}) and (C_{max}) are held constant while the (C_{ml}) is selected randomly from the distribution graph. (C_{ml}) are non-negative random variables which follow a triangle distribution. For this simulation, we used MATLAB and Vose ModelRisk software [19], both tools allow configurable simulations with a very large number of runs and can generate thousands of scenarios for each set of uncertain inputs. ModelRisk uses a mathematical model for input variables and triangle distribution function given as:

$$f(x) = \frac{2(x - C_{min})}{(C_{ml} - C_{min})(C_{max} - C_{min})} \quad for\ C_{min} \leq x \leq C_{ml}$$

$$f(x) = \frac{2(C_{max} - x)}{(C_{max} - C_{ml})(C_{max} - C_{min})} \quad for\ C_{ml} \leq x \leq C_{max}$$

The simulated output is generated given the mathematical relationship with input variables, and the results provide predictive indicators to support decision-making processes. However, with Monte-Carlo, input variables for the simulation model are uncertain, random and defined according to a probability distribution in order to capture and model those uncertainties. In this model, what happens is that thousands of scenarios are generated to reflect a probabilistic output for each uncertain input, according to triangle distribution, then, the resultant output values are computed thousands of times over again during the simulation. However, in order to obtain a convergence and more realistic values, a recommended run of 10,000

simulations is required, 1000 iterations being the barest minimum acceptable [20]. We generate 50,000 simulation runs, the model output is a probabilistic range of values and scenarios associated with security breach costs, as well as the probability distribution associated with those values.

6 Simulation Results and Discussion

Results of Monte Carlo simulation shown in figure 4 add an extra dimension to the initial deterministic values. As the simulation begins, samples are taken from each of the breach cost probability distribution. ModelRisk then computes the average random value at the end of each iteration. During the simulation, different scenarios are generated based on the frequency proportional to the probability of those scenarios occurring.

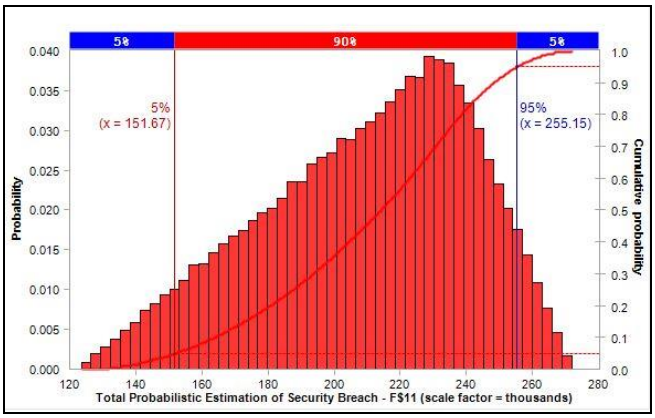

Figure 4: Simulation result in ModelRisk with cumulative overlay

At the end of the simulation, the output histogram represents 50,000 scenarios for security breach cost. The result of the simulation takes into account all uncertainties and it is in the form of probability distribution similar to the input parameters. These distributions represent possible outcomes, rather than single point predicted outcome.

From the model result in figure 4, it can be seen that the upper 5% and the lower 5% represents extreme cases that are ignored by the simulation output. From the parametric values in table 4, it can be seen that the total resource allocation could be as low as $123K or as high as $272K, but the realistic chance of resource allocation nearing these extreme values is very unlikely, hence the model ignored them. It can be seen that 90% of the simulation iterations fall under a value less than the upper bound estimated total values. Hence, we can say that 90% of the total allocation will meet our initial estimate. While this is not a guarantee, it allows us to adjust IT security budget to match the cost of potential breaches and also understand the risk that resource allocation may not meet initial estimates.

Further analysis of the result in figure 4 shows that given all the iteration of simulations, the absolute minimum value of $149,794 is much higher than the original deterministic lower bound value of $123k. Similarly, the absolute maximum probabilistic value of $253k after iteration is much lower than the deterministic value of $272k, with only 5% chance of the allocation going over the upper boundary. The most likely point estimate is around the value of $290k; from the location of the peak of the distribution, it can be seen that this value is rather more realistic than the deterministic value of 234,383. However, the cost of impact could be significantly higher, possibly twice as high in terms of cumulative percentage.

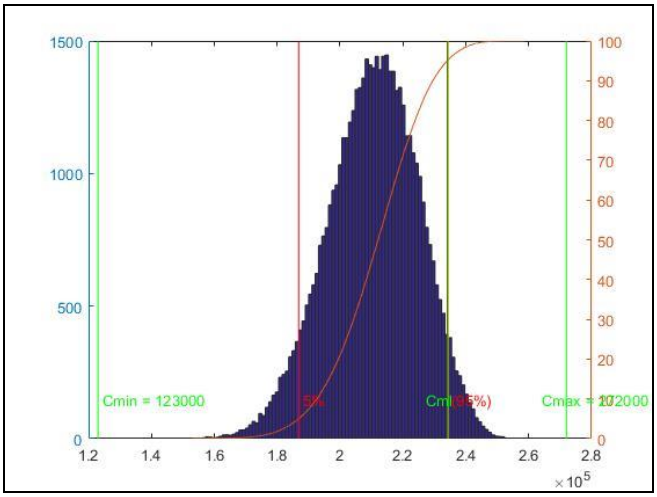

Figure 5: Simulation result in MATLAB showing values for C_{min} and C_{max}

In an attempt to validate our model, we compared the result with another simulation in MATLAB shown in figure 5, using the same input parametric values. The invariant that holds in both states of the models is that extreme values are ignored in the output of both simulations. While both models follow a similar distribution, it can be seen that not only did both simulations ignore lower and upper bound values, but also shows higher C_{min} and lower C_{max} than the deterministic values. This also confirms the correctness of the representation entities behaviour.

7 Conclusion

In general, predictive models allow us to make more useful and less erroneous decisions. Making important decisions without diligent consideration to uncertainties in the budgeting process can lead to unrealistic values. Forecasting with accuracy, on how much damage a successful security breach can cause is a real challenge for risk managers, especially when multiple assets and associated threat exposure are considered. Again, three point estimates, for all assets tend to become unreliable as the complexity of

asset classes in the model increases. Using probabilistic simulation, therefore, simplifies the complexity of cost estimation processes. The application of Monte Carlo simulation to information security investment decision, in particular, allows us to visualise different probabilistic outcomes in view of what might go wrong; given best case, worst case and most likely case scenarios.

MC allows us to understand the outcome of scenarios and help to understand unexpected pattern without necessarily exposing information assets to real threats. The output of Monte Carlo simulation is a range of values and risk assessor can derive confidence level from that range. It is expected that predictive models will enable management to make more effective decisions, and be part of the analytical input for policy formation If there is a sound understanding of what might go wrong, decision makers can utilise the model to implements appropriate risk mitigation strategies and budget allocation for security investment.

This study will be expanded as part of future work to include resource allocation for different information assets. A model that breaks down security budgets into fragments for further allocation, such that, information assets with the highest frequency and impact of threat events are allocated more resources than low impact events.

References

1. Steinbart, P. J., et al. (2015). "SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs." Journal of Information Systems.
2. ENISA (2012), Introduction to Return on Security Investment: Helping CERTs Assessing the Cost of (Lack of) Security Investment. [available] https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport [accessed] 15/04/16
3. Demetz, L. and D. Bachlechner (2013). To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool. The Economics of Information Security and Privacy, Springer: 25-47.
4. Gordon, L. A. and M. P. Loeb (2006). "Budgeting process for information security expenditures." Communications of the ACM 49(1): 121-125.
5. Cox, J. L. A. (2009), "Game Theory and Risk Analysis." Risk Analysis 29(8): 1062-1068.
6. Burtescu, E. (2012), "Decision Assistance in Risk Assessment-Monte Carlo Simulations." Informatica Economica 16(4): 86-92.
7. David Vose (1997), Monte-Carlo Risk Analysis Modelling. In Vlasta Molak ed. Fundamentals of Risk Analysis and Risk Management, CRC Press Inc. pp 57 – 78.
8. RiskAMP (2016), Risk Analysis using Monte Carlo Simulation, Whitepaper, [available at] http://www.riskamp.com/files/Risk%20Analysis%20using%20Monte%20Carlo%20Simulation.pdf [accessed 28 January 2016].
9. Böhme, R. (2010). Security Metrics and Security Investment Models. In Advances in Information and Computer Security (pp. 10-24). Springer Berlin Heidelberg.
10. Franqueira, V. N., Houmb, S. H., & Daneva, M. (2010). Using real option thinking to improve decision making in security investment. In On the Move to Meaningful Internet Systems: OTM 2010 (pp. 619-638). Springer Berlin Heidelberg.
11. Mizzi, A. (2010). Return on Information Security Investment - The Viability of an Anti-Spam Solution in A Wireless Environment. IJ Network Security, 10(1), 18-24.
12. Wang, S. L., Chen, J. D., Stirpe, P. A., & Hong, T. P. (2011). Risk-neutral evaluation of information security investment on data centres. Journal of Intelligent Information Systems, 36(3), 329-345.
13. Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114(2), 793-804.
14. Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. Journal of Research and practice in Information Technology, 38(1), 45-56.
15. Tallau, Linda J., Manish Gupta, and Raj Sharman. "Information security investment decisions: evaluating the Balanced Scorecard method." International Journal of Business Information Systems 5.1 (2009): 34-57.
16. Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis [available] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF [accessed] 14/03/16
17. Kaspersky Lab (2015) Damage Control: The Cost of Security Breaches, IT Security Risks Special Report Series [available] http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf [assessed] 12/03/16
18. Dan Lyon (2014), Modelling security investment with Monte-Carlo Simulations, The SANS Institute InfoSec Reading Room.
19. Van Hauwermeiren M and Vose D (2009). A Compendium of Distributions. [ebook]. Vose Software, Ghent, Belgium. [Available] www.vosesoftware.com. [Accessed] 29/09/16.
20. Turim, J. (1999). "Should We Risk It? David M. Kammen and David M. Hassenzahl, Princeton University Press, Princeton, New Jersey, 1999." Risk Analysis 19(5): 1017-1017.

21. Chinn, D., Kaplan, J., & Weinberg, A. (2014). Risk and responsibility in a hyperconnected world: Implications for enterprises. McKinsey Co.

22. Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. Decision Support Systems, 75, 49-62.

23. Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers. IEEE Security & Privacy, 14(3), 52-60.

24. Rue, R., Pfleeger, S. L., & Ortiz, D. (2007, June). A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. In WEIS.

25. Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage? Management Science, 54(4), 657-670.

26. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469.

27. Lee Bell et al. (2016) TalkTalk hack: ICO fines TalkTalk a record £400,000 for data breach [available] http://www.itpro.co.uk/security/24136/talktalk-hack-ico-fines-talktalk-a-record-400000-for-data-breach [accessed] 23/09/2016.

28. Graham Cluley (2016) Six months on from the TalkTalk hack - how has the firm suffered? [available] https://www.grahamcluley.com/talktalk-hack/ [accessed] 23/09/2016

29. Calder, A. and Watkins, G. (2010) 'Information Security Risk Management for ISO270001-270002', IT Governance Publishing, Cambridgeshire.

30. General Accounting Office (1999) 'Information Security Risk Assessment - Practices of Leading Organizations', A Supplement to GAO's May 1998 Executive Guide on Information Security Management. GAO/AIMD-00-33ions.

31. ISO/IEC 27001:2013 Information technology - Security techniques - Specification for an Information Security Management System. The British Standard Institute 2014.

32. Fagade, T., & Tryfonas, T. (2016). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 128-139). Springer International Publishing.

33. Fabrizio Baiardi, Fabio Corò, Federico Tonelli, Daniele Sgandurra, Automating the assessment of ICT risk, Journal of Information Security and Applications, Volume 19, Issue 3, July 2014, Pages 182-193, ISSN 2214-2126, http://dx.doi.org/10.1016/j.jisa.2014.04.002.

34. Baiardi, F. and D. Sgandurra (2013). "Assessing ICT risk through a Monte Carlo method." Environment Systems and Decisions 33(4): 486-499.

35. Bamakan, S. M., & Dehghanimohammadabadi, M. (2015). A Weighted Monte Carlo Simulation Approach to Risk Assessment of Information Security Management System. International Journal of Enterprise Information Systems (IJEIS), 11(4), 63-78. doi:10.4018/IJEIS.2015100103

36. Conrad J.R., Oman P., Taylor C. (2005) Managing Uncertainty in Security Risk Model Forecasts with RAPSA/MC. In: Dowland P., Furnell S., Thuraisingham B., Wang X.S. (eds) Security Management, Integrity, and Internal Control in Information Systems. IFIP International Federation for Information Processing, vol 193. Springer, Boston, M