Cybersecurity Economics – Balancing Operational Security Spending

Ekelund, S. & Iskoujina,

DOI 10.1108/ITP-05-2018-0252
ISSN 0959-3845

Publisher: Emerald

Cybersecurity Economics – Balancing Operational Security Spending

Abstract

Purpose – The purpose of this paper is to demonstrate how to find the optimal investment level in protecting an organisation's assets.

Design/methodology/approach – This study integrates a case study of an international financial organisation with various methods and theories in security economics and mathematics, such as value-at-risk (VaR), Monte Carlo simulation, exponential and Poisson probability distributions. Thereby it combines theory and empirical findings to establish a new approach to determining optimal security investment levels.

Findings – The results indicate that optimal security investment levels can be found through computer simulation with historical incident data to find value at risk (VaR). By combining various scenarios, the convex graph of the risk cost function has been plotted, where the minimum of the graph represents the optimal invest level for an asset.

Practical implications – The results can be used by leading business practitioners to assist them with decision making on investment to the increased protection of an asset.

Originality/value – The originality of this research is in its new way of combining theories with historical data to create methods to measure theoretical and empirical strength of a control (or set of controls) and translating it to loss probabilities and loss sizes.

Keywords – cyber security, security economics, security investment level, loss probability, control effectiveness measurement.

Paper type – Research paper

1 Introduction

Cybersecurity economics is an area concerned with whether an organisation is spending enough on securing their assets and whether the security budget is spent on the right things (Anderson and Schneier 2004). While there has been a significant increase in research on cybersecurity economics (for example, Jacobs, Bulters and van Wieren, 2016; Buith, 2015; Choudhry and Wong, 2013; Brecht and Nowey, 2012), the in-depth understanding of the security level, investments in security controls, and improvements for new controls need to be examined further.

Brecht and Nowey (2012) have categorised security spending by a proposed model for quantifying security costs that they argue will increase accuracy, objectivity and comparability. Defence costs are what an organisation has chosen to invest to protect their assets. Gordon and Loeb (2006) claim that the benefits from cybersecurity investments come from cost-savings related to the avoidance of potential incidents; the outcome of the potential losses from incidents; the loss probability, and the loss reduction from an investment. A different approach has been presented by Lee et al. (2011) who identified which security investment levels are optimal in terms of balancing costs of protection and risks to an asset. They argue that the security level can be viewed as the strength or effectiveness of the controls applied to protect an asset (Lee et al., 2011). Therefore, it is vital to understand the marginal strength improvement of the security level, and how it translates to the reduced loss probability when investing in an additional security control. NIST (National Institute of Standards and Technology) (2008) provides a guide for performance measurement for information security, but fundamentally lacks a method for measuring effectiveness of a given security level. Peláez (2010) suggests an approach to measure how much a control decreases the loss probability and link risk to the effectiveness of control. While Peláez (2010) provides guidance on how to measure effectiveness using a quantitative technique, it lacks a clear linkage to determine loss probabilities and marginal improvements for new controls.

The Basel Committee on Banking Supervision (2005) organised by Bank of International Settlements (BIS) are the regulator of the well-known Basel regulatory framework for financial institutions. This framework includes risk measurement using value-at-risk (VaR) for capital preservation purposes to secure banking operations in difficult times, defining VaR as the sum of expected and unexpected losses. Also Jacobs et al. (2016) present an approach to determine future loss probability by using Cyber VaR, a risk quantification method for cyber risks adapted from the framework proposed by World Economic Forum (2015). Cheung and Powell (2012) also examine how to calculate VaR using Monte Carlo simulation methods, where a stochastic process replaces the need to specify the probability distribution. Monte Carlo simulation is used in this study to determine VaR.

As seen, despite an increasing amount of research on cybersecurity economics, the question for cybersecurity practitioners as to how much to invest in protecting an organisation's information assets remains. Therefore, the research objective for this study is to examine how an organisation can determine how much it is recommended to invest in the protection of a digital information asset. To reach this objective, this paper will address the following three research questions: (i) How can defence costs be determined, and losses calculated? (ii) How can the effectiveness of a security control be measured in terms of reduction in future loss probability? (iii) How can cybersecurity investment aimed at protecting an asset be optimised? The paper begins by briefly reviewing the literature on cybersecurity economics in such areas as security costs, loss probability, effectiveness of security controls and investment optimisation. These areas are discussed in order to develop research propositions that will be tested before the findings are presented.

2 Theoretical background

2.1 Costs of the cyber defence effort

Investment in defence costs and security controls are aimed at protecting the assets of an organisation; when this fails, costs related to damages and losses are incurred (Wang et al, 2008). These two cost streams are explored to understand better how to categorise and quantify such costs. For example, Brecht and Nowey (2012) established a model for quantifying cyber security costs for increasing accuracy, objectivity and comparability. Their criterion for cost-benefit-calculation (Brecht and Nowey, 2012) are as follows: a) costs for managing information security (in this research referred to as defence cost), b) costs related to information security measures (in this research referred to as defence cost), c) costs incurred by information security incidents (in this research referred to as losses), and d) cost of capital induced by information security risks (considered outside scope of this research). Subsequently, Brecht and Nowey (2012) suggest the ISMS-Layers approach to information security cost quantification, which takes the perspective of information security management. According to ISO (n.d.), ISMS (Information Security Management System) is a risk management process involving people, processes and technology in protecting organisations' assets. Brecht and Nowey (2012) discuss measurement, determinability (difficulty in security attribution) and information security cost ratio (percentage attributed to security).

The ISMS-Layers approach appears adequate in determining information security costs. The security cost ratio, however appealing, is less helpful as one must anticipate substantial variations between organisations. Operational measures are assumed to be direct costs and the other layers to be indirect costs. Therefore, to assess the cost-benefit of an asset's defence, further investigation on how defence costs can be determined, and losses calculated is needed. This will be examined in the Research Question 1: How can defence costs be determined, and losses calculated? The research question will be tested through the following propositions (Figure 1):

> Proposition 1a: Direct defence costs can be defined as any security cost that is exclusively aimed at protecting one or more, but not all, assets.
>
> Proposition 1b: Indirect defence costs can be defined as any security cost that is aimed at protecting all assets.
>
> Proposition 1c: Defence cost can be shared between some or all assets, or between security and non-security budgets.
>
> Proposition 1d: Cost of damages and losses caused by a cyber incident can be categorised in short and long-term losses.

2.2 Determining effectiveness of a security control

The purpose of measuring the effectiveness of security controls is to understand how a set of applied controls translate to a loss probability, and particularly the marginal improvement of adding one to a set of controls is already in operation. Ideally, improvements may be expressed in terms of impact of VaR. NIST (National Institute of Standards and Technology) (2008) and Peláez (2010) provide approaches but fail to link to loss probabilities and marginal improvements for new controls. Pagett and Ng (2010) argue that standards-based IT governance models such as COBIT, NIST and ISO27004 are more focused on 'what' needs to be measured rather than 'how'. In response they propose an information security effectiveness framework to address the 'how', with effectiveness measured based on characteristics of a control (Pagett and Ng, 2010).

To measure effectiveness this way seems promising, but the proposal is leaning on what a designated policy prescribes, such as how many computers have antivirus installed. What if the policy is imperfect, but the characteristics otherwise score fully? This may lead an organisation to be lulled into a false sense of security. The method proposed increases understanding on how the effectiveness of a security control can be measured, but it does not link to a loss probability nor to VaR. By contrast, the approach presented by Huang et al. (2008) is more geared toward finding the optimal investment level where a security incident is associated with a probability function p that leads to losses. They further

claim that beyond some point of adding new controls, "the utility of the investment to the firm would actually be smaller than the expected utility from potential security breach" (Huang et al. 2008: 11). Moreover, Wang et al. (2008), Lee et al. (2011) and Huang et al. (2008) present solid mathematical models in deriving the expected value and VaR at a given security level, but the marginal effectiveness of adding a security control in terms of strength or effectiveness score is not covered.

In summary, the research has identified several approaches attempting to express effectiveness of security controls. However, as they lack solid numerical representations, they are not particularly useful for this research. There may, however, be opportunities for syntheses between the approaches. It is therefore necessary to further explore how the effectiveness of a security control is measured and linked to loss probability. Therefore, Research Question 2 in this paper will address how the effectiveness of a security control can be measured in terms of reduction in future loss probability. This research question will be tested through the following propositions (Figure 1):

> Proposition 2a: The reduction in loss probability is measurable and based on the characteristics of the security control, i.e. the effectiveness.
>
> Proposition 2b: The reduction measure is impacting VaR.

2.3 Determining optimal security investments

Faced with an opportunity to invest in more protection, it is beneficial to understand how to calculate the benefits from security investments and get guidance on how to find the optimal level to invest. Gordon and Loeb (2006) claim that cost-savings are an outcome of the potential losses from incidents, the loss probability and its reduction from an investment. They propose an approach to determine the optimal level of investment by a loss probability function with an investment level and a vulnerability level. Expected losses are given by the product of threat probability and monetary losses to an asset. The calculation may be conducted without historical attack data, that is, the investment level is the only decision variable. However, the vulnerability level and expected losses still need to be derived somehow. By contrast, Huang et al. (2008) discuss the use of expected utility theory to identify the security investment level that maximises the utility of the investment. The framework presented is similar to the one Gordon and Loeb (2002) used but with different boundary conditions and assumptions. To compute the optimal investment, the probability of a security incident occurring in a given time frame, an investment level, a potential loss and a risk-aversion coefficient must be determined. This approach (Huang et al., 2008) applies classical economic theories to compute an optimal security investment to protect

an asset. As an input, historical data to determine the loss probability is needed, as well as a risk-aversion coefficient.

The approaches reviewed are useful contributions in understanding the optimal amount to invest in security. They are not, however, particularly beneficial on their own as they require input variables such as loss probabilities, vulnerability level and risk-aversion coefficients, which are not straightforward to determine. In effect, these approaches must be combined with supplemental methods to deal with the more demanding input variables. Therefore, Research Question 3 will examine how a cybersecurity investment aimed at protecting an asset can be optimised. This research question will be tested through the following proposition (Figure 1):

> Proposition 3a: The optimal investment level can be expressed as the minimum sum of defence costs and losses to an asset.

2.4 Theoretical framework

The theoretical framework is a model consisting of the factors and their relationships that contribute to a problem and prepares for further discussions and investigation. It helps postulate and test certain relationships in order to improve our understanding (Sekaran 2003). The theoretical framework in this case has been created from the hypotheses identified above: that the risk cost – the sum of defence costs and losses – has a minimum value that can be identified by adding or subtracting controls; increasing defence cost should proposedly reduce the losses (VaR), but it is also dependant on the effectiveness of the control invested in. The variables used in the framework are therefore one dependant variable, the risk cost, with underpinning independent variables. From the findings and interpretations of the literature review, the dependant variable has been identified as minimum risk cost as the measure of "how much to invest". The dependent variable, key independent variables and their interconnections are illustrated in
Figure 1.

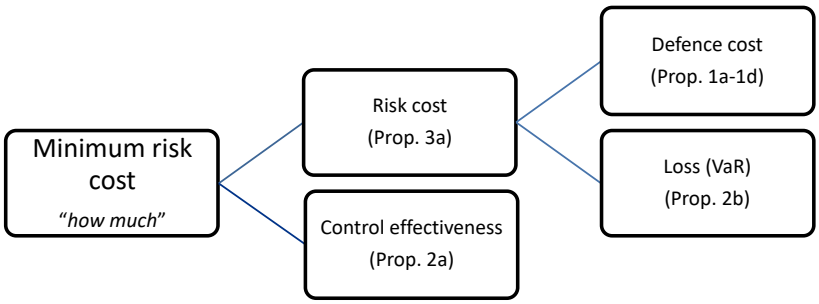


Figure 1. Theoretical framework

3 Research methodology

This research is based on the scientific method, which is a systematic approach towards observing phenomena, drawing conclusions and testing hypothesis (Sekaran 2003). Building and testing theories from a case study is a strategy that is used as a complementary method; developing theories and propositions from such empirical evidence is one of the best bridges from qualitative evidence to deductive research (Eisenhardt and Graebner, 2007). Kulmala et al (2006:147) deployed this approach arguing that "a single case study was selected because initial understanding on the studied phenomenon was the target"; Shih et al (2017) based their research on a case study arguing its suitability for investigating contemporary phenomena, which aligns well with the nature of this research. The general problem statement - how much an organisation should invest in protection - induces the need for researching existing knowledge in a set of multi-disciplinary topics. The identification of gaps in existing knowledge generate this study's research questions, which in turn generates the propositions. To answer each proposition, qualitative or quantitative research is conducted. The propositions are created in alignment to the theoretical framework, as illustrated in Figure 2.

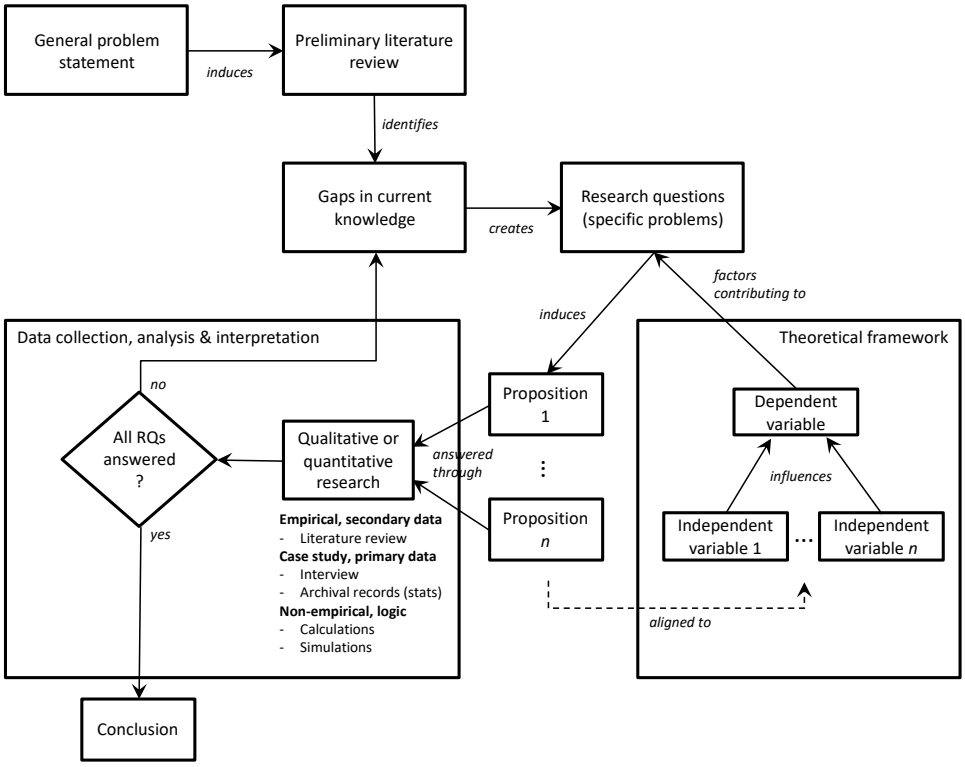


Figure 2. Research approach, derived from Sekaran (2003: 56)

The research questions are addressed using a case study with a mixed method. The qualitative approach serves as an input to a quantitative approach, which in turn will be used to acquire answers to the research questions. The data was collected through interviews and archival records. The case study took place at an anonymised international financial services organisation referred to as 'FinCorp Ltd.', a substantial player in the European market and with offices around the world. During the course of 6 weeks, three leaders from the information security department were interviewed, which in turn relayed many of questions to various subordinates for supporting information and provision of archival data. This department was chosen as it has overall responsibility for the protection of information assets. The interviews were conducted through plenary sessions. The participants were the CISO (Chief Information Security Officer), the head of security architecture and the head of risk management. To set the stage, the first session was initiated by asking how security investments are justified today. Subsequently, questions were asked and discussed sequentially. The questions were sent a day in advance of the two sessions arranged. The objective of data analysis is to meet the research objective, and therefore the most important aspect of data evaluation is to convert the data collected into a format which will support adequate inference and decision-support (Sreejesh et al. 2014). Where appropriate, data is converted into a numerical format appropriate for calculations and simulations.

Computer-based simulation uses mathematical models to determine effects of change and has been used to study risk management in the finance area for some time (Sekaran 2003). Particularly when considering VaR, Monte Carlo simulation – an algorithm randomly simulating outcomes based on historical data – is the preferred method for data analysis for two reasons: to take advantage of any historical distribution of risk factors (Chourdry 2013), and to join a discrete distribution (loss arrivals) with a continuous one (loss sizes) (Navarrete 2006). The simulation starts with initial values for annual loss occurrence probability, and the loss sizes' mean and standard deviation from the collected data. Then new arrival and size data are simulated by randomisation and joined to create new 12-months loss scenarios. The approach is illustrated in Figure 3.

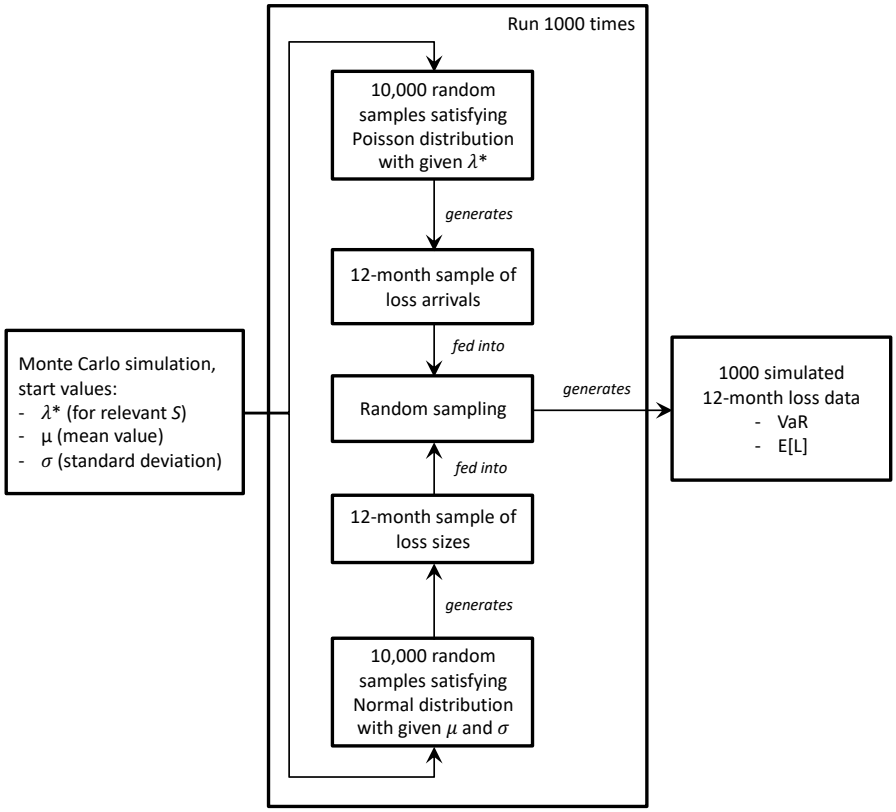


Figure 3. Monte Carlo simulation model

4 Data analysis, findings and discussion

4.1 Proposition 1a. Direct defence costs can be defined as any security cost that is exclusively aimed at protecting one or more, but not all assets.

Direct costs are costs directly associated with security controls protecting an asset; "if the asset is removed, the controls and their associated costs are detachable", as one interviewee put it. Furthermore, a security control may protect more than one asset (but not all) but still constitute direct costs. FinCorp Ltd. has deployed four security controls with the following annual operation costs to (directly) protect A_π:

Table 1. Deployed security controls at FinCorp Ltd

No	Security control	Estimated annual operation cost
1	End-user with antivirus	£ 0
2	Application firewall	£ 600,000
3	Two-factor authentication	£ 200,000
4	Fraud detection module	£ 300,000

When considering the cost of cyber security, both defence cost and losses are considered as suggested by Brecht and Nowey (2012). As argued by Gordon and Loeb (2002) and Huang et al. (2008), the level of defence cost is related to the losses. It is therefore beneficial to cover these two cost categories in concept to monitor their interaction. Identifying what represent direct costs of protecting an asset is a matter of agreeing on what to include in such calculations. Based on the data collected from FinCorp Ltd., this research considers the direct defence cost as Operational Measures (as per the ISMS-Layers approach in Figure 4), and the other categories as indirect costs. In general, the defence costs are represented as an annual cost that include an initial investment cost, an annual operating cost, and depreciation expenses due to a limited useful lifetime.

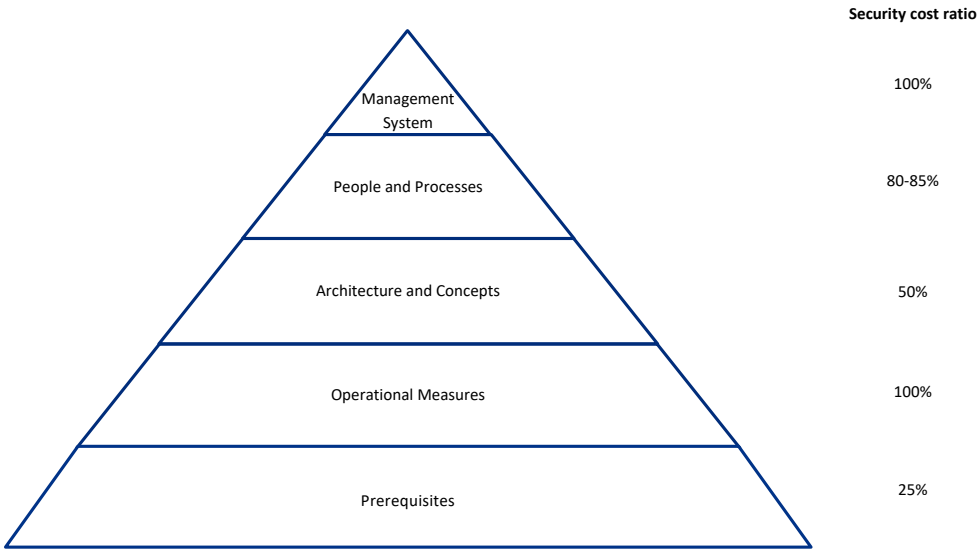


Figure 4 - ISMS-Layers approach with ratios (Brecht and Nowey 2012, p.15) with adjustment

Consider a set of security controls $\{n_1, n_2, \ldots\}$ protecting an asset $A_i \in \mathcal{P}$. Each control, denoted node, has a cost, $c(n) > 0$. Further, view this set of nodes as forming a risk vector, denoted $v(A_i)$. The concept of a risk vector will be formally defined and discussed below, but for now it is sufficient to

realise that each node has an individual cost and thus the cost of vector $v(A_i)$, denoted $c(v(A_i))$, is the cost of all nodes protecting it.

4.2 Proposition 1b. Indirect defence costs can be defined as any security cost that is aimed at protecting all assets.

Indirect costs are, as expressed during the interviews, "costs that are incurred by all employees with part or full-time responsibility for information security, security policies and guidelines, security awareness and training, and the ISMS". The estimated annual indirect costs of protecting all assets at FinCorp Ltd. including protect A_π, are categorised as follows:

Table 2. Information security cost categories

No	Security cost category	Estimated annual indirect cost
1	Cost of operating the management system	£ 1,000,000
2	Cost of people and processes	£ 2,000,000
3	Cost of architecture and concepts	£ 250,000
4	Cost of prerequisites	£ 500,000

The obtained indirect cost data aligns well with the cost categories defined by Brecht and Nowey (2012). Let Ω be the total annual information security cost of an organisation in protecting its portfolio of assets $\mathcal{P} = \{A_1, A_2, \ldots, A_k\}$. Also, let ψ be the direct annual defence cost and ω the indirect annual cost, or expressed more formally:

$$\Omega = \omega + \psi = \omega + c(v(A_1)) + c(v(A_2)) + \ldots + c(v(A_k)) \quad (1)$$

Further assume $\psi = c(v(A_1)) + c(v(A_2)) + \ldots + c(v(A_k))$, where $\psi_1 = c(v(A_1)), \ldots, \psi_k = c(v(A_k))$. In contrast to Brecht and Nowey (2012), ψ is considered to be 100% dedicated to information security according to the definition of a risk vector, see 4.5. The formula for indirect costs ω is exhibited in Figure 5:

	Cost of Management System * 1
+	Cost of People and Process * 0.85
+	Cost of Architecture and Concepts * 0.5
+	Cost of Prerequisites * 0.25
=	ω

Figure 5. Formula for indirect costs

The indirect annual cost ω_{A_π} of protecting A_π is exhibited in Figure 6:

	Cost of Management System * 1	= £ 1,000,000
+	Cost of People and Process * 0.85	= £ 2,000,000
+	Cost of Architecture and Concepts * 0.5	= £ 250,000
+	Cost of Prerequisites * 0.25	= £ 500,000
=	Total indirect costs ω_{A_π}	= £ 3,750,000

Figure 6. Indirect cost of protecting Aπ

The obtained indirect cost ω_{A_π} is valid only if asset A_π is the only asset. There are, however, more assets in FinCorp's possession. It is therefore necessary to investigate how direct and indirect costs are shared (see the next Proposition 1c).

4.3 Proposition 1c. Defence costs can be shared between some or all assets, or between security and non-security budgets

The case study obtained information on several nodes including all that are used to protect asset A_π, that is $n_i \in v(A_\pi)$. Table 5 in Section 4.5 displays the nodes and their annual operation costs.

The total number of assets in FinCorp's possession were not obtained from the case study but, using the asset as a service approach, the case study participants anticipated it to be less than 10. As per the case study, a node n can be protecting several assets. Therefore, the node cost $c(n)$ should be divided between all the assets being protected by that node. This "reuse" of nodes is thus beneficial from a cost standpoint but may not be so from a protection standpoint as a defeated node may cause collateral damage. It is not, however, considered in the scope of this research to explore this potential weakness further.

Let $\overline{n_k} \geq 1$ be the number of "reuses" a node k has in protecting assets in $\mathcal{P}$. The direct annual cost $\psi_i = \mathrm{c}(\nu(A_i))$ for protecting asset $A_i \in \mathcal{P}$ is thus:

$$\psi_i \;=\; \mathrm{c}(\nu(A_i)) \;=\; \frac{c(n_1)}{\overline{n_1}} + \cdots + \frac{c(n_k)}{\overline{n_k}} \tag{2}$$

Also, when considering the indirect annual cost ω, the cost may be equally divided between the assets in the portfolio $\mathcal{P}$. For an asset $A_i \in \mathcal{P}$ the indirect annual cost is:

$$\omega_i = \frac{\omega}{Number\ of\ assets\ in\ \mathcal{P}} \tag{3}$$

At FinCorp Ltd. the direct annual costs of protecting A_π are illustrated in Table 1. Applying these to (2), the direct defence cost of $c(\nu(A_\pi))$ is obtained:

$$\psi_{A_\pi} = \mathrm{c}(\nu(A_\pi)) = \frac{c(n_1)}{\overline{n_1}} + \frac{c(n_2)}{\overline{n_2}} + \frac{c(n_3)}{\overline{n_3}} + \frac{c(n_4)}{\overline{n_4}} =$$

$$= \frac{0}{1} + \frac{£600{,}000}{4} + \frac{£200{,}000}{1} + \frac{£300{,}000}{1} = £\,650{,}000 \tag{4}$$

Further assume that FinCorp Ltd. has five assets in total, then the indirect cost ω_{A_π} is obtained through:

$$\omega_{A_\pi} \;=\; \frac{£\,3{,}750{,}000}{5} \;=\; £\,750{,}000 \tag{5}$$

In summary, the total annual cost of protecting A_π by applying (2) and (3) is:

$$\Omega_{A_\pi} = \psi_{A_\pi} + \omega_{A_\pi} = £\,650{,}000 + £\,750{,}000 = £\,1{,}400{,}000$$

Based on this, an annual level of defence cost has been calculated. For this level of defence, FinCorp Ltd. experienced losses of £ 491,825 over a period of 30 months (see the next Proposition 1d).

4.4 *Proposition 1d. Cost of damages and losses caused by a cyber incident can be categorised in short and long-term losses.*

The Information Security Department at FinCorp Ltd. may or may not be representative in their response to what is more important: short-term or long-term losses following a security incident. As the department is being measured on short-term data, this was considered most important. Loss observations, caused by 54 incidents, were provided for a period of 30 months. The losses incurred, £ 491,825 in total, were short-term losses caused by cyber-attacks.

Long-term losses, such as those arising from loss of competitive advantage, missing growth opportunities, and loss of customers themselves, were by contrast hard to determine within the time allocated by the study. They are therefore omitted from this research. It is, nevertheless, considered plausible to find persons and even whole departments that value long-term losses above short-term losses. The loss observations that took place in this study are what Jacobs et al. (2016) consider as operational continuity and payments; typical short-term losses affecting daily income and cash flow. These figures can be used for further calculations and simulations to investigate how defence costs and cost of losses are connected, and how future loss probability can be derived. To study this further, there is a need to construct a function denoted *risk cost*, which will take both the defence cost and the losses into account.

Risk cost. The asset value of A_π was estimated to £ 240,000,000. At the defence level Ω = £ 1,400,000, losses worth £ 491,825 were incurred, yielding a 12-month average of £ 196,730. Assume a new node is added aimed at protecting A_π with some cost $c(n) > 0$. One would expect losses to be reduced by an amount x. However, adding another similar node with the same cost will reduce the losses by less than x, i.e. $x - y_1$. And another similar node will thus reduce the losses by $x - y_2$ where $y_2 < y_1$. This is in alignment with that the marginal improvement on security decreases with higher investments, where at some point "the utility of the investment to the firm would actually be smaller than the expected utility from potential security breach" (Huang et al. 2008: 11). This can be generalised through the following function:

$$\text{Risk cost} = \text{defence cost} + \text{losses} \tag{6}$$

According to the extreme value theorem (Renze and Weisstein n.d.) the risk cost function will have a maximum and minimum and create a U-shaped graph as illustrated in Figure 7. This is supported by Lee et al. (2011) claiming that the risk cost function is continuous and convex (u-shaped). Inspired by its shape, it is referred to as the U-graph of an asset. By construction, it follows that all assets have

a U-graph, i.e. a minimum risk cost exists for all assets. Thus, this graph is suitable to depict if an increased investment in defence is worthwhile.

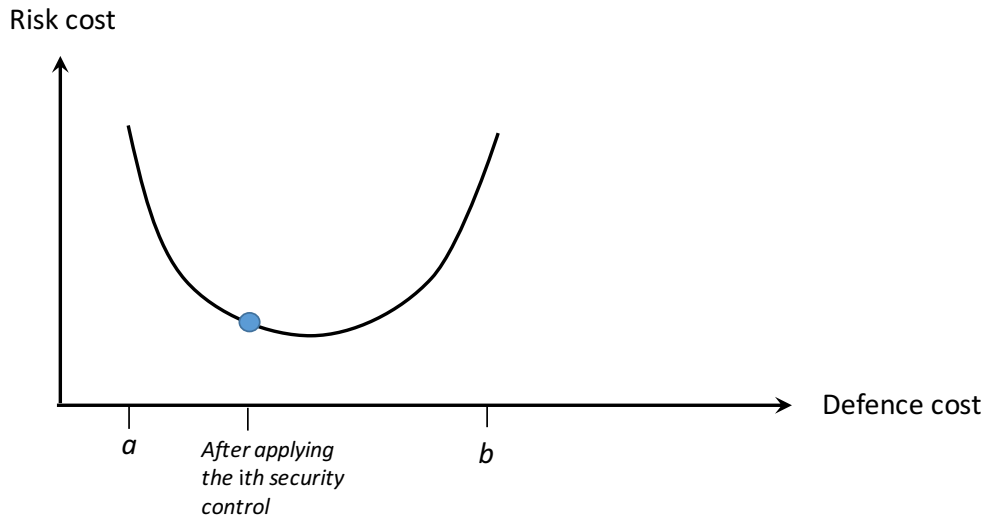


Figure 7. U-graph (risk cost function) of an asset

Since risk is about a future event that may or may not occur, and the example above is referring to incurred losses, there is a need to be a little more specific. Three variants of risk cost can be identified as described in Table 3.

Table 3. Risk cost variants

Risk cost variant	**Variables**	**Formula**	**Purpose**
Incurred Risk Cost	Defence cost, Mean incurred losses	$IRC = \Omega + L$	The actual risk costs, given Ω
Expected Risk Cost	Defence cost, Expected losses	$ERC = \Omega + E[L]$	How the expected future risk costs will be, given Ω
VaR Risk Cost	Defence cost, VaR	$VRC = \Omega + VaR$	What the maximum future risk costs with a given confidence level will be, given Ω

VaR calculation for determining future loss. To collect data for the U-graph of A_π, it is necessary to calculate future losses in terms of expected loss and VaR. It is also necessary to find a way to determine the effectiveness of the security controls and translate them into quantitative values and explore how this will affect the loss probabilities. As suggested by the World Economic Forum (2015), Jacobs et al. (2016), Wang et al. (2008), Lee et al. (2011) and Huang et al. (2008), VaR can be applied for determining future losses. Based on the data obtained from FinCorp Ltd. VaR can be calculated for the online services asset A_π employing a Monte Carlo simulation in R. Initially, it is assumed that no historical data exist. The simulation follows the steps described in Figure 3, and the code for the computation is shown in Figure 8, where each step is followed by a description.

Monte Carlo method - using R

```
### Initial values
asset_value <- 240000000                                  # asset value
mmean = -0.0068                                           # average observed monthly losses as percentage
msd = 0.0168                                              # standard deviation of observed monthly losses as percentage

### Monte Carlo Simulation - normal distribution
samples <- 10000                                          # sample size
result <- rnorm(samples,mean=mmean,sd=msd)                # random generation of normally distributed values
sorted_result <- sort(result)                             # sort the result vector

VaR95m_percent <- sorted_results[as.integer(runs * 0.05)] # Get the element that represents monthly 95% VaR value in %
VaR95y_percent <- VaR95m_percent * sqrt(12)                # Calculate annual 95% VaR value in %

### Calculate and print the VaR monetary values
VaR95m_value <- round(abs(VaR95m_percent * asset_value) / 100, digits=0)   # Monthly monetary value
VaR95y_value <- round(abs(VaR95y_percent * asset_value) / 100, digits=0)   # Annual monetary value

### Print the results
print(paste("Mean VaR month:" VaR95m_value, " (", round(VaRm_percent, digits=3),"%)"))
print(paste("Mean VaR year :" VaR95y_value, " (", round(VaRy_percent, digits=3),"%)"))

[1] "Mean VaR month: 82706    ( -0.034 %)"
[2] "Mean VaR year : 286504   ( -0.119 %)"
```

Figure 8. VaR calculations with Monte Carlo simulation

Subsequent simulations take advantage of the actual historical distribution for the risk factor rather than assuming a pre-determined normal distribution (see 4.6). Many simulations are run, each yielding different results. In the end, the simulation will aggregate to a more realistic result (Choudhry 2013). By using the mean (μ) and standard deviation (σ) derived from the loss observations, the 5% VaR loss value is obtained: VaR = £ 82,706 per month. This indicates that there is a 5% probability of losing more than £ 82,706 in the next month as a result of cyber incidents, or £ 286,504 over the next 12 months. The expected value of a normal distribution is its mean value (Hildebrand n.d.), thus:

$$E[L] = \mu = | - 0.0068\% \cdot £\ 240{,}000{,}000 | = £\ 16{,}320 \text{ per month}$$

Thus, FinCorp Ltd. can expect to lose on average £ 16,320 per month or £ 195,840 per year, by construction approximately the same as the average losses incurred. Applying these numbers to the risk cost variants yields:

Table 4. Risk cost calculations 1

Risk cost variant	**Calculation**
IRC	= £ 1,400,000 + £ 196,730 = £ 1,596,730
ERC	= £ 1,400,000 + £ 195,840 = £ 1,595,840
VRC	= £ 1,400,000 + £ 286,504 = £ 1,686,504

4.5 Proposition 2.a. The reduction in loss probability is measurable and based on the characteristics of a security control, i.e. the effectiveness.

One of the key points in this research is to demonstrate how to depict the U-graph for an asset. This will be shown by using A_π as an example. Consequently, a method to determine the effectiveness of a node, both alone and in union with a set of existing ones, is needed. As the literature review did not increase our understanding as to how to determine such effectiveness, this research demonstrates a possible approach.

Inspired by the attack-defence process articulated by Jacobs et al. (2016), and paths of attacks (aka attack vectors), a simple framework for visualising and exploring the effectiveness of nodes can be created, referred to as a risk vector. This research assumes the term risk vector for the pathway where incidents leading to malicious exploitation may occur with potential to cause losses. It is correspondingly along this pathway where security controls are applied, and their effect can be measured, e.g. reduction in loss amounts. To illustrate how the malicious exploitation of an asset occurs, consider the cyber kill chain (Lockheed, n.d.) depicted in Figure 9.

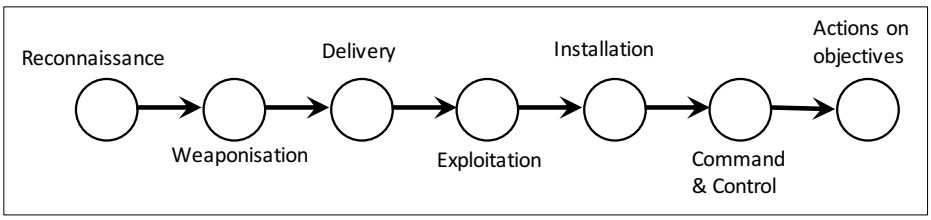


Figure 9. Cyber kill chain (Lockheed, n.d.)

Signs of a security incident are considered as either precursors or indicators, where the former is a sign that an incident may occur in the future and the latter is a sign that an incident is ongoing or has already occurred (NIST 2012). The prime interest is in the precursors and indicators appearing along the vector. A complementary view is the attack-defence process, describing attack flow and an organisation's cyber defence capability (Jacobs et al 2016) as illustrated in Figure 10.

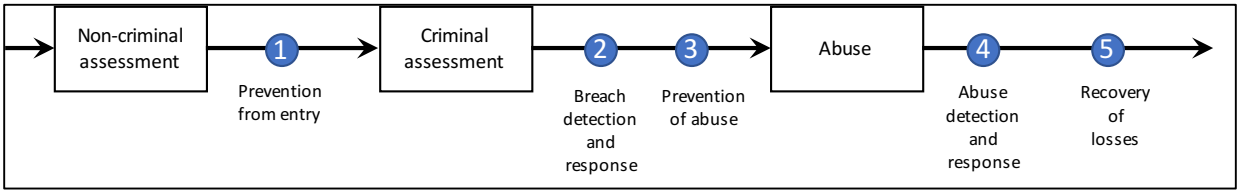


Figure 10. Attack-defence process (Jacobs et al 2016, p.150)

The relation between the two views is shown in Figure 11, offering an illustration of a risk vector.

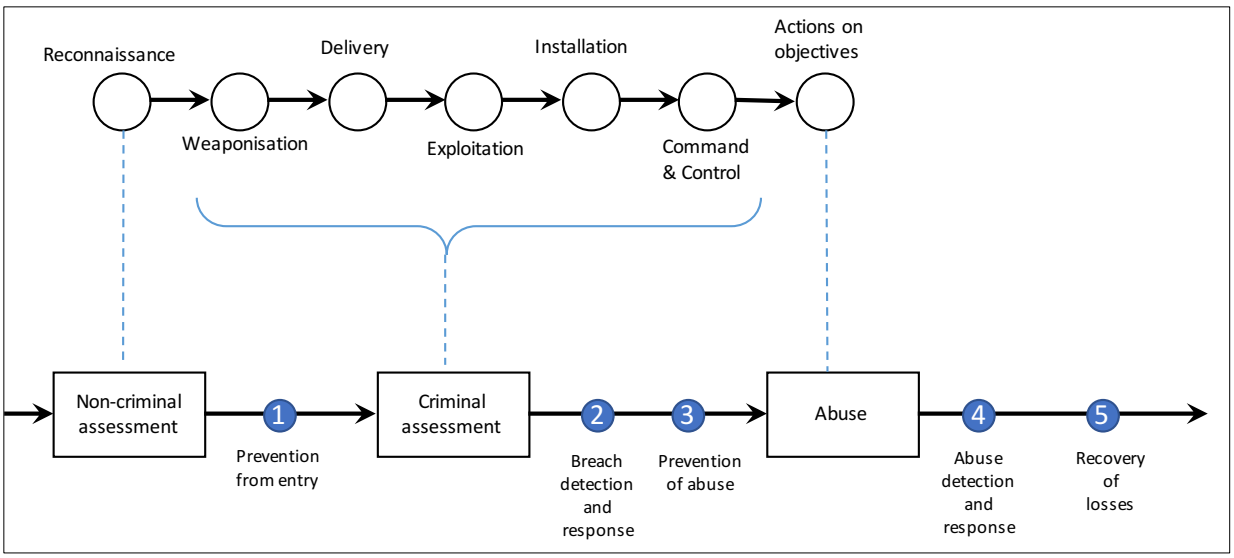


Figure 11. Relation between the cyber kill chain (Lockheed, n.d.) and the attack-defence process (Jacobs et al 2016, p.150)

In a vector $v = v(A)$, consider a node $n \in v$ with a strength, $\rho(n) > 0$ which is derived from a score, $s(n) \geq 0$, according to the control effectiveness scoring scheme discussed below. Thus, $v(A)$ will have a cumulative cost denoted $c(v(A))$ or simply $c(v)$ if it is clear which asset it pertains to. Likewise, $v(A)$ will have a cumulative strength denoted $\rho(v(A))$ or simply $\rho(v)$. The strength will be a measure on how much all nodes will reduce the risk of loss to an asset A. The following risk vector $v(A_\pi)$ was observed at FinCorp Ltd:

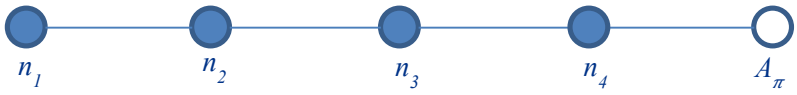


Figure 12. Risk vector $v(A_\pi)$ at FinCorp

where the nodes identified are:

Table 5. Nodes protecting A_π

Node	Security control	Estimated annual operation cost
n_1	End-user with antivirus	£ 0
n_2	Application firewall	£ 600,000
n_3	Two-factor authentication	£ 200,000
n_4	Fraud detection module	£ 300,000

Through the construct of the risk vector, a framework for measurement and modelling of risk has been established. The literature review did not, however, identify any complete method of measuring a security control's effectiveness alone or in concert with other controls in protecting an asset, and even less so linking effectiveness to loss probabilities. Nevertheless, Pagett and Ng (2010) argue that the effectiveness is linked to the characteristics of a control. Thus, a purpose-built approach is needed.

Control effectiveness and strength. A security control instantiates a mitigation treatment strategy such as deterrence, prevention, detection or recovery, aiming to reduce the likelihood and/or impact of a risk (Straub and Welke 1998). Peláez (2010) argues that ISO/IEC 27004 provides guidance for measuring the effectiveness, not only the of controls themselves, but also management and implementation processes, commonly referred to as the Information Security Management System (ISMS). Based on this, consider the nature of the control (type), its mean of functioning (prescription), its susceptibility to being defeated (fallibility) and its ability to adapt to new threats (agility) as characteristics that impact its effectiveness. It is thus possible to assess a control's effectiveness against its capability in deterrence, prevention, detection and recovery. Assessing these factors may also implicitly measure the effectiveness of the treatment strategy. Figure 13 illustrates the scoring scheme:

Score / Characteristic	1	2	3	4
Type	Administrative	Administrative/ technncal	Technical/ administrative	Technical
Prescription	Logging only/ observation	Rules/signature/ heuristics	Live threat intelligence	Machine learning
Fallibility	Likely	Possible	Unlikely	Impossible
Agility	Reprogramming	Re-configuration	Run-time	Self-learning

Figure 13. Control effectiveness scoring scheme

By rating the control against these characteristics an effectiveness score s can be determined. For each characteristic, a score of 4 is strongest and 1 is weakest. A characteristic that is not applicable is scored as 0. That gives a possible scoring range $0 \leq s \leq 16$ for each control, and the sum of effectiveness scores of all controls in the risk vector $v(A)$ is simply:

$$S = S(v(A)) = \sum s_i \qquad S \geq 0, \quad i = 0, 1, 2, \ldots \tag{7}$$

Applying the scoring scheme to the nodes in $v(A_\pi)$ is illustrated in Figure 14, and the selected rating marked with green. The result of applying (9) to these scorings is $S = 9 + 11 + 9 + 11 = 40$.

n_1. End-user with AV. **Score: 9**

Characteristic \ Score	1	2	3	4
Type	Administrative	Administrative/ technical	Technical/ administrative	**Technical**
Prescription	Logging only/ observation	**Rules/signature/ heuristics**	Live threat intelligence	Machine learning
Fallibility	Likely	**Possible**	Unlikely	Impossible
Agility	**Reprogramming**	Re-configuration	Run-time	Self-learning

n_2. Application firewall. **Score: 11**

Characteristic \ Score	1	2	3	4
Type	Administrative	Administrative/ technical	Technical/ administrative	**Technical**
Prescription	Logging only/ observation	**Rules/signature/ heuristics**	Live threat intelligence	Machine learning
Fallibility	Likely	**Possible**	Unlikely	Impossible
Agility	Reprogramming	Re-configuration	**Run-time**	Self-learning

n_3. Two-factor authentication. **Score: 9**

Characteristic \ Score	1	2	3	4
Type	Administrative	Administrative/ technical	Technical/ administrative	**Technical**
Prescription	Logging only/ observation	**Rules/signature/ heuristics**	Live threat intelligence	Machine learning
Fallibility	Likely	**Possible**	Unlikely	Impossible
Agility	**Reprogramming**	Re-configuration	Run-time	Self-learning

n_4. Fraud detection module. **Score: 11**

Characteristic \ Score	1	2	3	4
Type	Administrative	Administrative/ technical	Technical/ administrative	**Technical**
Prescription	Logging only/ observation	**Rules/signature/ heuristics**	Live threat intelligence	Machine learning
Fallibility	Likely	**Possible**	Unlikely	Impossible
Agility	Reprogramming	Re-configuration	**Run-time**	Self-learning

Figure 14. Control scoring of nodes in $v(A_\pi)$

Adding a security control to protect an asset reduces the risk of that asset. The key question is how much and how this relates to S. To answer this, another heuristic method will be applied assuming that the marginal improvement on security decreases with additional controls (Huang et al 2008). As an introduction, one can use intuition to depict a reasonable trajectory that resonates with probability, i.e. taking on values in the interval [0, 1].

To depict this trajectory in accordance with the security level as proposed by Lee et al. (2011), and in such a way that it can be linked to probability, consider the exponential probability distribution with a scale parameter τ (Taboga 2010):

$$f(x) = e^{-\tau x} \qquad x \in [0, \infty) \tag{8}$$

and particularly the cumulative density function:

$$F(x) = 1 - e^{-\tau x} \qquad x \in [0, \infty) \tag{9}$$

This function will always generate a value in the interval from [0, 1]. By substituting x with the control effectiveness score S, and applying it to (9), the following is achieved:

$$F(S) = 1 - e^{-\tau S} \qquad S \in [0, \infty) \tag{10}$$

By assigning an appropriate initial value to the scale parameter τ, the control effectiveness score to strength conversion function is finalised. For example, let:

$$\tau = 0.05 \tag{11}$$

This results in the following trajectory:

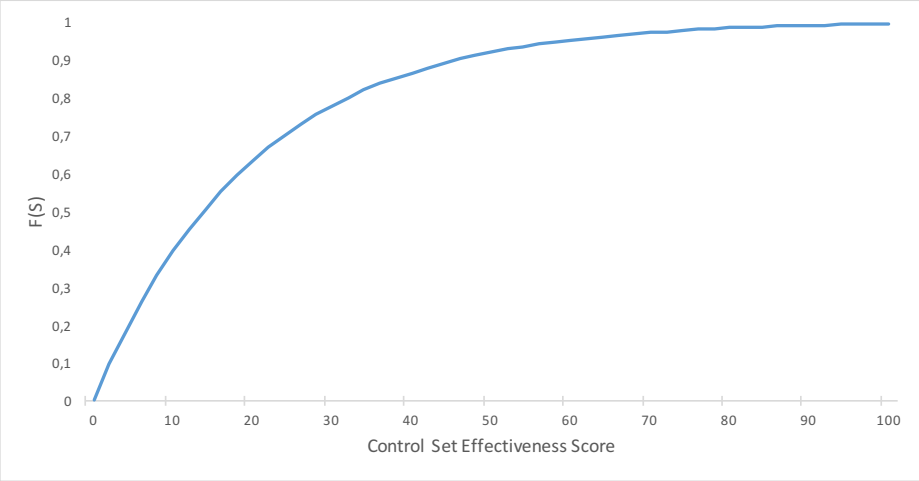


Figure 15. Control effectiveness score

This trajectory aligns well with the decreasing marginal effect and should serve the purpose for converting the security control effectiveness score to a strength metric ρ. This research thus defines strength of vector ν as:

$$\mathrm{F}(S) = \rho(\nu) = 1 - e^{-\tau S} \qquad S \in [0, \infty) \tag{12}$$

Table 6 presents some calculations applying (11) with (12) including the effectiveness scoring of $v(A_\pi)$:

Table 6. Samples of conversion between effectiveness and strength scores

S	$\rho(v)$
0	0
10	0,39
20	0,63
30	0,78
40	$\rho(v(A_\pi))$ = **0,86**
50	0,92
100	0,99

The next step is to establish a link between strength $\rho(v)$ and a desirable risk metric of $v(A)$: the probability for a loss occurrence on asset A along risk vector $v(A)$, referred to as loss probability. Marchini (2008) argues that a Poisson distribution is a discrete probability distribution for the counts of events that occur randomly in a given time interval; a counting process. Consider the discrete random variable X representing losses occurring through $v(A)$; the arrival of these occurrences can be viewed as a counting process as each arrival is independent of each other, and thus has a Poisson distribution. If λ is the mean number of observed loss occurrences per day, then the probability of observing x events on a given day is determined by the following distribution function (Mikosch 2009):

$$p(X = x) = e^{-\lambda} \frac{\lambda^x}{x!} \qquad x = 0, 1, 2, 3, \ldots \tag{13}$$

It follows that the cumulative distribution function is given by:

$$F(X = x) = \sum_{i=0}^{x} e^{-\lambda} \frac{\lambda^i}{i!} \tag{14}$$

By the law of large numbers, if one has $N(t)$ events occurring during time t, λ is determined through (Mikosch 2009):

$$\lambda = \frac{N(t)}{t} \tag{15}$$

The positive real number λ also happens to be equal to the expected value of X and its variance (Mikosch 2009):

$$\lambda = E[X] = Var[X] \tag{16}$$

FinCorp Ltd. endured 54 loss occurrences over a 30-month period, a mean of 1.8 losses per month, i.e.

$$\lambda_m = 1.8 \qquad \text{loss probability, per month} \tag{17}$$

which by (16) is also the expected value going forward. Then the following cumulative probability function is obtained:

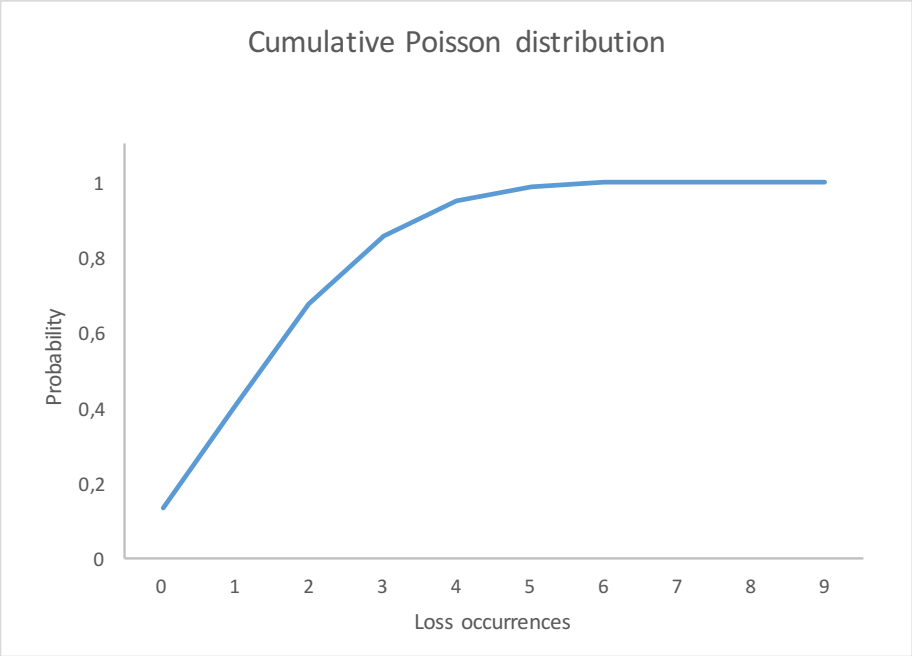


Figure 16. Cumulative Poisson distribution for loss occurrences at FinCorp Ltd.

The trajectory of a cumulative Poisson distribution function resembles that of the cumulative exponential probability distribution; this neighbouring similarity will be used to approximate a link

between the strength and the mean loss probability λ. From (17) $\lambda_m = 1.8$ for a month was found, thus a one-day (1/30 of a month) time horizon yields:

$$\lambda_d = 0.06 \qquad \text{loss probability, per day} \tag{18}$$

By design, the closer to 1 the strength $\rho(\nu)$ moves, the closer to 0 the loss probability moves. The following construct articulates exactly this point, where ε is some error adjustment factor:

$$\lambda_d = 1 - \rho(\nu) \cdot \varepsilon \tag{19}$$

Recall from (12) that $\rho(\nu) = 1 - e^{-\tau S}$. As an adjustment factor is already in place, the scale parameter τ, one can simply combine (12) and (19):

$$\lambda_d = e^{-\tau S} \tag{20}$$

If the effectiveness score of a risk vector and the scale parameter τ are determined, these produce an estimator for the mean number of loss occurrences. Conversely, once historical data has been collected, the mean λ_d can be easily computed and the scale parameter τ assigned an appropriate value. By rearranging (20) the following is obtained:

$$\tau = -\frac{\ln(\lambda_d)}{S} \tag{21}$$

This finalises the heuristic model for the relationship between the strength $\rho(\nu)$ and the mean loss probability λ_d. For risk cost calculations, an adjustment of the calculations based on the new scale parameter τ is needed. Then one must select a new prospective node, and run new calculations to determine the new losses. Consider an expansion of Table 6 with the new knowledge obtained from (18) and (21) to derive the new τ. In addition, the values for the scenarios of adding and subtracting up to two nodes are calculated. From Figure 14, an average effectiveness score of $s = 10$ is inferred. The new calculations are derived from the current situation as highlighted in green, i.e. with $\lambda_d = 0.06$:

Table 7. Adjustment calculations

		Initial calculation, $\tau = 0.05$		**New calculation, $\tau = 0.07$**	
	S	$\rho(\nu) = 1 - e^{-\tau S}$	$\lambda_d = 1 - \rho(\nu)$	$\rho(\nu) = 1 - e^{-\tau S}$	$\lambda_d = 1 - \rho(\nu)$
- 2 nodes	20	0.63	0.37	0.76	0.24
- 1 node	30	0.78	0.22	0.88	0.12
Current	40	0.86	0.14	0.94	0.06
+ 1 node	50	0.92	0.08	0.97	0.03
+ 2 nodes	60	0.99	0.05	0.99	0.01

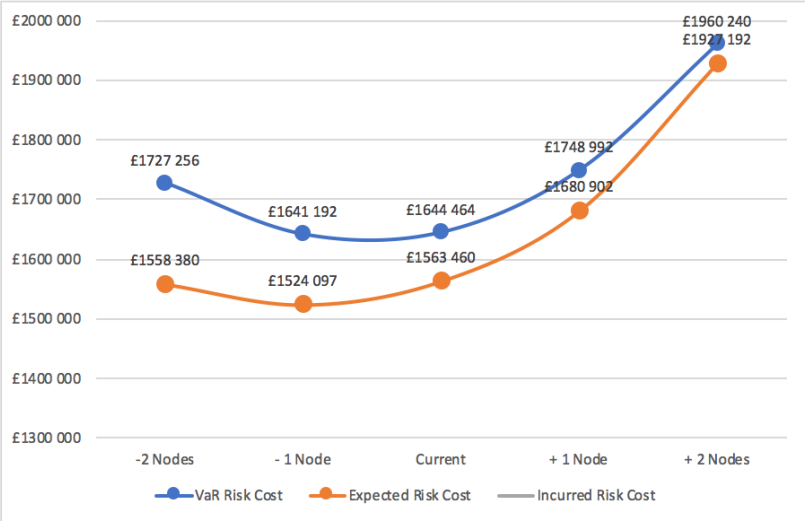
4.6 Proposition 2b. The reduction measure is impacting VaR.

No quantitative data was collected for this Proposition, but the discussion below elaborates logically on the knowledge created so far. To obtain the relevant points in the U-graph of A_π, Monte Carlo simulations must be run to compute the numbers. This is supported by Cheung and Powell (2012) claiming that the stochastic process of the Monte Carlo method replaces the need to specify the probability distribution. This research assumes that adding a node reduces the loss probability, and conversely, subtracting a node increases it (as per Table 7). Since only the loss probabilities at various levels of protection are known, this must be translated to loss sizes. Recall from (4) that the direct costs of protecting A_π come from four nodes. Consider the two-factor authentication and fraud detection module incurring a cost of £200,000 and £300,000 respectively. These nodes will be used for estimating Ω_{A_π} at various levels. The following steps are executed to obtain graph values:

Table 8. Process for obtaining values for U-graph

Step	Activity
1	Start with the current strength S = 40, which gives an annual mean $\lambda^* = \lambda_d \cdot 365 = 21.9$ to be used as input to the Monte Carlo simulation together with the mean and standard deviation for the normal distributed VaR calculation, μ = -0.0068 % and σ = 0.0168 %. The simulation will generate 1000 simulated values for: - Annual loss probability λ^* - 5% VaR loss for as percentage and value - Expected loss $E[L]$ as value
2	Compute mean values of λ^*, VaR and $E[L]$. Verify that mean λ^* is approximately the same as entered in step 1. For S = 40, also verify that the mean VaR ≈ £ 286,504 and $E[L]$ ≈ £ 195,840 (from 0) to ensure the simulation is reliable
3	Compute the defence cost. For S = 40, it is £ 1,400,000. For the other levels of S, use the cost £200,000 for the first node (both adding and subtracting), and £300,000 for the second node. Note: For simplicity, the indirect cost is assumed to be fixed although in reality it will vary somewhat with adding/subtracting controls
4	Compute VaR Risk Cost and Expected Risk Cost for S = 20, 30, 40, 50 and 60

The result from the simulation is illustrated in Figure 17, which incidentally shows that the risk reduction impacts VaR and therefore verifies this Proposition. An extract of the simulation results is presented in Appendix A.



	-2 Nodes	- 1 Node	Current	+ 1 Node	+ 2 Nodes
Strength *S*	20	30	40	50	60
Daily λ	0,24	0,12	0,06	0,03	0,01
Mean λ* (annual)	89,321	43,7372	21,869	10,9783	3,5933
Mean VaR month	£238 848	£127 296	£70 680	£42 984	£17 400
Mean VaR month %	-0,09952	-0,05304	-0,02945	-0,01791	-0,00725
Mean VaR year	£827 256	£441 192	£244 464	£148 992	£60 240
Mean VaR year %	-0,34469	-0,18383	-0,10186	-0,06208	-0,0251
E[L] year	£658 380	£324 097	£163 460	£80 902	£27 192
Defence cost Ω	£900 000	£1 200 000	£1 400 000	£1 600 000	£1 900 000
VaR Risk Cost	£1 727 256	£1 641 192	£1 644 464	£1 748 992	£1 960 240
Expected Risk Cost	£1 558 380	£1 524 097	£1 563 460	£1 680 902	£1 927 192
Incurred Risk Cost			£1 596 730		
Node cost	-£300 000	-£200 000		£200 000	£300 000

Figure 17. U-graph for A_π

The risk reduction is impacting VaR as demonstrated in the calculations. The immediate interpretation of the U-graph is that FinCorp Ltd. does not currently need to invest more in security as the risk cost would increase; there are presently no better investment choices, and the research has thereby also found the financially optimal investment level.

4.7 *Proposition 3a. The optimal investment level can be expressed as the minimum risk cost (sum of defence costs and losses) to an asset.*

Previously it was argued that the convex risk cost function exists for all assets and will form a U-graph. It is also shown that the minimum of this function will correspond to the financially optimal defence level for an asset, as demonstrated above. The approach resembles the model developed by Gordon and Loeb (2006) but expands it by using the U-graph as historical data is used to determine loss probability rather than just assuming it. Gordon and Loeb (2002) and Huang et al. (2008) present approaches that

identify the budget, but the strength must also be determined. By applying the approach from this research, a control having a cost within budget and a strength that reaps the most benefit can be identified. Combining models like those developed by Gordon and Loeb (2002) and Huang et al. (2008) with approaches described in this research would therefore reinforce each other in order to verify this.

5 Discussion

This research articulates an easily deployable approach to convey an organisation's risk posture in a continuous manner to top management. Through its scientific basis, it should therefore be considered more reliable as a decision-support tool than the prevalent "fear, uncertainty, and doubt (FUD) strategy" (Brecht and Nowey 2012: 2) used to sell investments in cybersecurity. This study has employed a combination of qualitative and quantitative techniques to expand the understanding of this topic.

Propositions 1a to 1d demonstrated how defence costs can be determined and categorised as direct and indirect. Defence costs can also be shared and categorised according to the ISMS-Layers approach (Brecht and Nowey, 2012) to prepare for a more realistic cost picture. Cost of damages and losses can be divided into short-term and long-term to prepare for loss calculations. The research has thus shown how cost of damages and losses can be categorised and by knowing both the defence cost and the correlated losses, the risk cost of an asset is determined. The risk cost function will for all assets be convex and form a U-graph. The findings and logical reasoning support existing knowledge. This answers Research Question 1: How can defence costs be determined, and losses calculated?

The risk vector framework was established to aid in visualising and exploring the effectiveness of security controls. Through the control effectiveness scoring scheme, the characteristics of a security control is quantified a correlated to loss probability for an asset. By applying the collected data to the proposed Monte Carlo simulation, it is demonstrated how the adding (or subtracting) of a security control to the risk vector impacts VaR and will generate a U-graph. The research has shown how the loss probability of an asset can be measured by the characteristics of the security controls protecting it. The findings and logical reasoning are connecting existing knowledge from different areas, creating a synthesis that expands the knowledge obtained from the literature review. This answers Research Question 2: How can the effectiveness of a security control be measured in terms of reduction in future loss probability?

The use of Monte Carlo simulation to generate U-graphs can be used as a generic method to identify the minimum of the U-graph by adding or subtracting security controls until it is located. As both defence costs and future losses are considered, this minimum will correspond to the financially

optimal defence level for an asset. Conclusively, the logical reasoning is connecting existing knowledge from different areas, creating a synthesis that expands the knowledge obtained from existing literature. This answers Research Question 3: How a cybersecurity investment can be aimed at protecting an asset be optimised?

To summarise, this research has demonstrated how to categorise information security costs; direct and indirect defence costs and losses. Direct costs can be identified through their dependency on one or more, but not all, assets. Otherwise, defence cost is regarded as indirect. It is also found that defence costs can be shared. For direct costs, this can be done between assets that are collectively being protected by a control, whereas indirect costs can be evenly distributed between all assets. By knowing both the defence cost and correlated losses, the risk cost of an asset is determined. The risk cost function will for all assets be convex and form a U-graph. The minimum of this function will correspond to the financially optimal defence level for an asset, obtained through calculating VaR for various scenarios. It has further been shown how loss probabilities of an asset can be measured through the controls' characteristics, linked to a strength score and adjusted by actual data. The risk amendment following the addition or subtraction of new controls in the risk vector is impacting VaR, which is demonstrated in the calculations and the U-graph. Finally, this research has shown that an organisation can balance its operational security spending by using the U-graph, so it supports the business leadership in making informed decisions on whether the defence spending is enough, too much or too little in protecting assets.

6 Conclusion

The research has verified and demonstrated how organisations can determine the optimal investment level in protecting assets, and the case study has been used as a verification of the theories articulated. By means of a multi-disciplinary scientific approach, the paper provides guidance to leading business practitioners to assist them with decision-making on cyber security. The approach can be integrated with existing risk management practices and strengthen business-case discussions and cyber security related communication with top management. By the adoption of this approach, an organisation can balance its operational security spending.

The limitations of the research include a modest number of loss observations from one case study, and the use of normal probability distribution. These areas should undergo further research including larger data set of losses and exploring other probability distributions. Furthermore, the approach

has limitations where there are no historical data available or the data has zero losses. Future research should therefore investigate how to integrate very low probability events with devastating impact.

7 References

Allan, N., Cantle, N., Godfrey, P., and Yin, Y. (2012) 'A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice'. *British Actuarial Journal,* Vol. 18, No. 1, pp.163-234.

Anderson, R. and Schneier, B. (2004) 'Economics of Information Security', available at https://www.schneier.com/academic/paperfiles/paper-economics.pdf/ (accessed 19 September 2018).

Andew, D.P.S., Pedersen, P.M., and McEvoy, C.D. (2011) *Research Methods and Design in Sport Management.* Human Kinetics, USA.

Atrill, P. and McLaney E. (2015) *Accounting and Finance for Non-Specialists*. Pearson, Harlow, UK.

Aven, T. (2013) 'On the Meaning and Use of the Risk Appetite Concept'. *Risk Analysis*, Vol. 33, No. 3, pp. 462-468.

Basel Committee on Banking Supervision (2005) 'An Explanatory Note on the Basel II IRB Risk Weight Functions' available at http://www.bis.org/bcbs/irbriskweight.pdf/ (accessed 16 February 2017).

Brecht, M. and Nowey, T. (2012) 'A Closer Look at Information Security Costs', available at https://www.econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf (accessed 19 September 2018)

Buith, J. (2015) 'The Benefits, Limits of Cyber Value-at-Risk'. *The Wall Street Journal,* 4 May, available at http://deloitte.wsj.com/cio/2015/05/04/the-benefits-limits-of-cyber-value-at-risk/ (accessed 19 September 2018).

Böhme, R. (ed.) (2013) *The Economics of Information Security and Privacy*. Springer, Berlin Heidelberg.

Cheung, Y. H., and Powell, R. J. (2012) 'Anybody can do Value at Risk: A Teaching Study using Parametric Computation and Monte Carlo Simulation'. *Australasian Accounting, Business and Finance Journal*, Vol. 6, No. 5, pp.101-118.

Choudhry, M 2013, Introduction to Value-at-Risk, John Wiley & Sons, Incorporated, New York. Available from: ProQuest Ebook Central. [19 September 2018]

Damodaran, A. (n.d.) 'Value At Risk (VAR)', available at http://www.stern.nyu.edu/~adamodar/pdfiles/papers/VAR.pdf/ (accessed 19 September 2018).

Dupuy, P. (2009) 'Pure Indicator of Risk Appetite'. *Australian Economic Papers*, Vol. 49, No. 1, pp.18-33.

Edwards, A. and Skinner, J. (2009) *Qualitative Research in Sports Management.* Taylor and Francis, Hoboken, available at https://ebookcentral.proquest.com/lib/coventry/reader.action?docID=535013/ (accessed 19 March 2017).

Eisenhardt, K. M. and Graebner, M. E. (2007) 'Theory Building from Cases: Opportunities and Challenges'. *Academy of Management Journal*, Vol. 50, No. 1, pp.25-32.

Gibb, F. and Buchanan, S. (2006) 'A framework for business continuity management'. *International Journal of Information Management,* Vol. 26, No. 2, pp.128-141.

Gordon, L.A. and Loeb, M.P. (2006) *Managing cybersecurity resources: a cost-benefit analysis.* McGraw-Hill, New York, USA.

Gordon, L.A. and Loeb, M.P. (2002) 'The economics of information security investment'. *ACM Transactions on Information and Systems Security,* Vol. 5, No. 4, pp.438-457.

Hildebrand, A.J. (n.d.) 'Math 408, Actuarial Statistics I', available at http://www.math.uiuc.edu/~ajh/370/408normal.pdf/ (accessed 19 September 2018).

Hyde, K. F. (2000) 'Recognising Deductive Processes in Qualitative Research'. *Qualitative Market Research: An International Journal*, Vol. 3, No. 2, pp.82-90.

Huang, C.D., Hu, Q., and Behara, R.S. (2008) 'An economic analysis of the optimal information security in the case of a risk-averse firm', available at https://www.researchgate.net/publication/223518357_An_economic_analysis_of_the_optimal_information_security_investment_in_the_case_of_a_risk-averse_firm/ (accessed 19 September 2018).

International Public Sector Accounting Standards (2006) 'Glossary of Defined Terms', available at https://www.ifac.org/system/files/publications/files/glossary-of-defined-terms-2.pdf/ (accessed 19 September 2018).

ISO (n.d.) 'ISO/IEC 27001 – Information security management', available at http://www.iso.org/iso/iso27001/ (accessed 19 September 2018).

ISO (2009) 'Information technology: Security techniques: Information security management: Monitoring, measurement, analysis and evaluation'. *ISO/IEC 27004:2009*. International Standard Organization, Geneva, Switzerland.

Jacobs, V., Bulters, J., and van Wieren, M. (2016). 'Modeling the Impact of Cyber Risk for Major Dutch Organizations'. in Koch, R. and Rodosek, G. (ed.) *Modeling the Impact of Cyber Risk*

for Major Dutch Organizations, 'European Conference on Cyber Warfare and Security' at Bundeswehr University, Munich, 7-8 July 2016. Reading: Academic Conferences International Limited

Kopparty, S. (2011) '*Trees',* available at http://www.math.rutgers.edu/~sk1233/courses/graphtheory-F11/trees.pdf/ (accessed 12 January 2017).

Kulmala, H.I., Ojala, M., Ahoniemi, L., and Uusi-Rauva,E. (2006) 'Unit cost behaviour in public sector outsourcing', *International Journal of Public Sector Management*, Vol. 19, No. 2, pp.130-149.

Lee, Y.J., Kauffman, R.J., and Sougstad, R. (2011) 'Profit-maximizing firm investments in customer information security'. *Decision Support Systems* 51 (4), 904-920.

Leitch, M. (2010) 'Making sense of risk appetite, tolerance, and acceptance', available at http://www.internalcontrolsdesign.co.uk/appetite/full.shtml/ (accessed 13 February 2017).

Lockheed M. (n.d.) 'The Cyber Kill Chain®', available at http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html/ (accessed 19 September 2018).

Marchini, J. (2008) 'Lecture 5: The Poisson Distribution', available at http://www.stats.ox.ac.uk/~marchini/teaching/L5/L5.notes.pdf/ (accessed 19 September 2018).

Mikosch, T. (2009) *Non-Life Insurance Mathematics*. Springer, Berlin, Heidelberg.

Navarrete, E. (2006) 'Practical Calculation of Expected and Unexpected Losses in Operational Risk by Simulation Methods'. *Banca & Finanzas: Documentos de Trabajo*, Vol. 1, No. 1, pp.1-12.

NIST (2014) 'Framework for Improving Critical Infrastructure Cybersecurity', available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf/ (accessed 19 September 2018).

NIST (2012) 'Computer Security Incident Handling Guide', available at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final (accessed 19 September 2018).

NIST (2008) 'Performance Measurement Guide for Information Security', available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf/ (accessed 19 September 2018).

O'Gorman, R. and MacIntosh, R. (2014) *Research Methods for Business and Management*. Goodfellow Publishers, Oxford, available at https://www.goodfellowpublishers.com/free_files/Contents%20and%20copyright-e9d3f30a12012dd4ec3c99d8684e1af8.pdf/ (accessed 19 September 2018).

The Open Group (2009) 'Risk Taxonomy', available at http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf (accessed 19 September 2018).

Pagett, J. and Ng, S. (2010) ‘Improving Residual Risk Management Through the Use of Security Metrics’, available at https://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Pagett_v2.pdf/ (accessed 19 September 2018).

Peláez, M.H.S. (2010) ‘Measuring effectiveness in Information Security Controls’, available at https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398/ (accessed 19 September 2018).

Pelnekar, C. (2011) ’Planning for and Implementing ISO 27001’. *ISACA Journal*, Vol.4, available at http://www.isaca.org/Journal/archives/2011/Volume-4/Documents/jpdf11v4-Planning-for-and.pdf/ (accessed 19 September 2018).

Renze, J. and Weisstein, E. W. (n.d.) ‘Extreme Value Theorem’, available at http://mathworld.wolfram.com/ExtremeValueTheorem.html/ (accessed 19 September 2018).

Security Scorecard (2016) ‘2016 Financial Industry *Cybersecurity Report’,* available at https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf/ (accessed 5 April 2017).

Sekaran, U. (2003) *Research Methods for Business: A Skill Building Approach.* John Wiley & Sons, Danvers, MA, USA.

Shih, Y.-W., Wu, Y.-L., Wang, Y.-S., and Chen, C.-L. (2017) ‘Investigating the post-adoption stage of Voice over Internet Protocol (VoIP) telephony diffusion: A use-diffusion approach’, *Information Technology & People*, Vol. 30, No. 4, pp.753-784.

von Solms, R. and van Niekerk, J. (2013) ’From information security to cyber security’. *Computers & Security,* Vol. 38, pp.97-102.

Sreejesh, S., Mohapatra, S., and Anusree, M.R. (2013) *Business Research Methods,* Cham: Springer International Publishing, available at https://ebookcentral.proquest.com/lib/coventry/detail.action?docID=1398578 (accessed 12 February 2017).

The Stationary Office (2011) ‘ITIL® Managing Digital Information Assets’, available at http://www.nationalarchives.gov.uk/documents/information-management/itil-white-paper-2011.pdf/ (accessed 27 February 2017).

Straub, D. W., & Welke, R. J. (1998) ‘Coping with systems risk: Security planning models for management decision making’. *Management Information Systems Quarterly, Vol.* 22, No. 4, pp.441-469.

Taboga, M. (2010) ‘Lectures on probability and statistics’, available at https://www.statlect.com/probability-distributions/Poisson-distribution/ (accessed 19 September 2018).

Wagner, S.M. and Neshat, N. (2010) ‘Assessing the vulnerability of supply chains using graph theory’. *Internal Journal of Production Economics*, Vol. 126, No.1, pp. 121-129.

Wang, J., Chaudhury, A., and Rao, H.R. (2008) ‘A Value-at-Risk Approach to Information Security Investment’. *Information Systems Research,* Vol. 19, No. 1, pp.106-123.

World Economic Forum (2015) ‘Partnering for Cyber Resilience, Towards the Quantification of Cyber Threats’, available at http://www3.wefo-rum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf/ (accessed 19 September 2018).

8 Appendix A

Result tables from Monte Carlo simulation

1000 runs were conducted, and the mean numbers are calculated based on this. For brevity, only the first 10 rows are displayed.

				λ = 0.24 / -2 nodes				
Run	Lambda(y)	VaR month	VaR month %	VaR year	VaR year %	E[L]	# simulation runs	1000
0	91,42	261600	-0,109	907200	-0,378	686058	Mean λ	89,32
1	87,42	230400	-0,096	799200	-0,333	647596	Mean VaR month	238848
2	89,42	240000	-0,1	830400	-0,346	674565	Mean VaR month %	-0,0995
3	91,92	249600	-0,104	864000	-0,36	659558	Mean VaR year	827256
4	83,08	225600	-0,094	782400	-0,326	608591	Mean VaR year %	-0,3447
5	87,92	232800	-0,097	806400	-0,336	645161	E[L]	658380
6	88	235200	-0,098	813600	-0,339	653118		
7	88,25	240000	-0,1	830400	-0,346	653918		
8	90,83	249600	-0,104	864000	-0,36	670633		
9	89,75	242400	-0,101	840000	-0,35	664841		
10	86,08	223200	-0,093	772800	-0,322	636782		
				λ = 0.12 / -1 node				
Run	Lambda(y)	VaR month	VaR month %	VaR year	VaR year %	E[L]	# simulation runs	1000
0	46,25	141600	-0,059	489600	-0,204	331424	Mean λ	43,74
1	43,67	129600	-0,054	448800	-0,187	332090	Mean VaR month	127296
2	45,75	132000	-0,055	458400	-0,191	323079	Mean VaR month %	-0,0530
3	42	124800	-0,052	432000	-0,18	314727	Mean VaR year	441192
4	45,17	129600	-0,054	448800	-0,187	334286	Mean VaR year %	-0,1838
5	45,42	132000	-0,055	458400	-0,191	324656	E[L]	324097
6	44,17	129600	-0,054	448800	-0,187	345787		
7	43,5	124800	-0,052	432000	-0,18	342080		
8	45,75	129600	-0,054	448800	-0,187	344152		
9	40,83	120000	-0,05	415200	-0,173	308502		
10	43,67	122400	-0,051	424800	-0,177	314700		
				λ = 0.06 / current				
Run	Lambda(y)	VaR month	VaR month %	VaR year	VaR year %	E[L]	# simulation runs	1000
0	22,67	72000	-0,03	249600	-0,104	156737	Mean λ	21,87
1	22	69600	-0,029	240000	-0,1	143268	Mean VaR month	70680
2	21,75	64800	-0,027	225600	-0,094	177715	Mean VaR month %	-0,0295
3	19,92	64800	-0,027	225600	-0,094	157021	Mean VaR year	244464
4	24,58	76800	-0,032	266400	-0,111	171338	Mean VaR year %	-0,1019
5	20,75	64800	-0,027	225600	-0,094	164337	E[L]	163460
6	23,33	74400	-0,031	256800	-0,107	160603		
7	21,92	72000	-0,03	249600	-0,104	153439		
8	18,67	62400	-0,026	216000	-0,09	176444		
9	17,75	57600	-0,024	199200	-0,083	162013		
10	22,67	76800	-0,032	266400	-0,111	168629		
				λ = 0.03 / +1 node				
Run	Lambda(y)	VaR month	VaR month %	VaR year	VaR year %	E[L]	# simulation runs	1000
0	12,67	60000	-0,025	208800	-0,087	77173	Mean λ	10,98
1	10,85	40800	-0,017	141600	-0,059	72171	Mean VaR month	42984
2	10,52	45600	-0,019	158400	-0,066	79716	Mean VaR month %	-0,01791
3	11,83	50400	-0,021	175200	-0,073	67200	Mean VaR year	148992
4	11,35	43200	-0,018	148800	-0,062	79990	Mean VaR year %	-0,06208
5	10,33	45600	-0,019	158400	-0,066	81538	E[L]	80902
6	10,93	45600	-0,019	158400	-0,066	81199		
7	10,59	40800	-0,017	141600	-0,059	84569		
8	11,43	45600	-0,019	158400	-0,066	74118		
9	11,01	40800	-0,017	141600	-0,059	81237		
10	12,16	50400	-0,021	175200	-0,073	85279		
				λ = 0.01 / +2 nodes				
Run	Lambda(y)	VaR month	VaR month %	VaR year	VaR year %	E[L]	# simulation runs	1000
0	3	14400	-0,006	50400	-0,021	26750	Mean λ	3,59
1	3,42	16800	-0,007	57600	-0,024	22156	Mean VaR month	17400
2	3,58	16800	-0,007	57600	-0,024	27619	Mean VaR month %	-0,00725
3	3,33	16800	-0,007	57600	-0,024	22984	Mean VaR year	60240
4	3,5	16800	-0,007	57600	-0,024	12457	Mean VaR year %	-0,0251
5	3,5	16800	-0,007	57600	-0,024	31243	E[L]	27192
6	3,08	16800	-0,007	57600	-0,024	29150		
7	2,58	12000	-0,005	40800	-0,017	27422		
8	3,67	19200	-0,008	67200	-0,028	23095		
9	4,42	19200	-0,008	67200	-0,028	28769		
10	3,33	14400	-0,006	50400	-0,021	17740		