Lessons on Catastrophe: Modelling a Relationship between Credit Ratings and Cyber Insurance Risk

Rob Champion

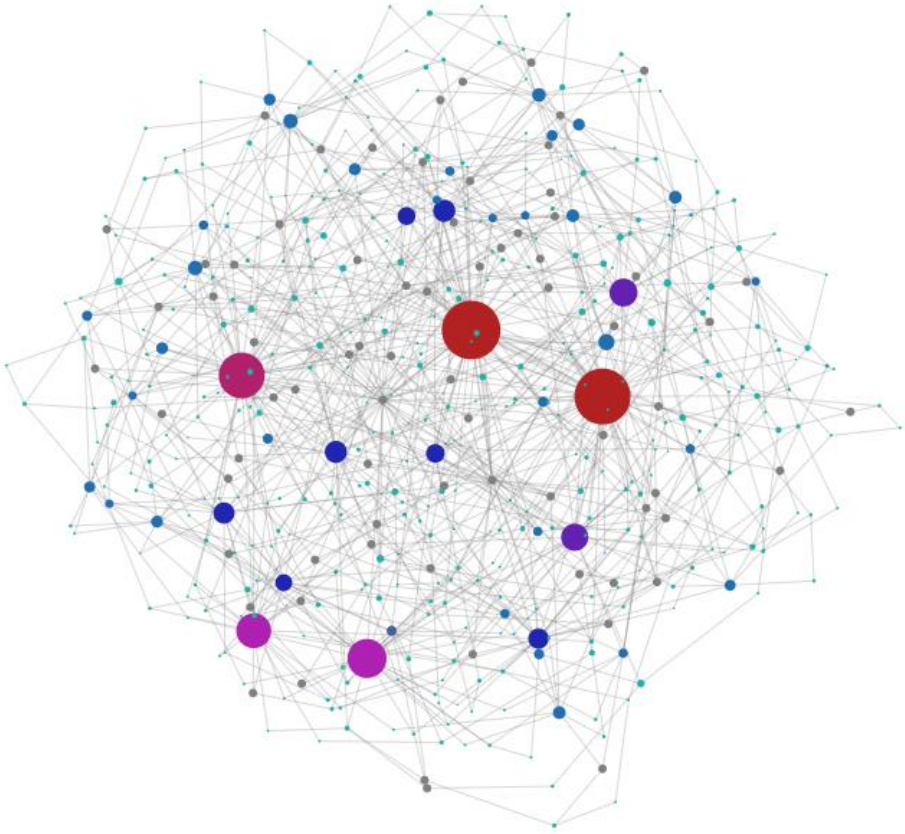
Technical Report

RHUL–ISG–2020–2

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Lessons on Catastrophe: Modelling a Relationship between Credit Ratings and Cyber Insurance Risk



Name: Robert Champion

Student Number: 100910017

Supervisor: Carlos Cid

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature: Date:

Table of Contents

Table of Figures & Tables

Acknowledgements

To Rachel and my family who've all been incredibly supportive of my studies and career change, as well as willingly subjected to my writing.

I would also like to thank Tom Pountney and his colleagues at Besso for providing their experience of the insurance industry.

"All models are wrong, but some are useful."

~ George Box

"The best material model for a cat is another, or preferably the same cat."

*~ (Rosenbleuth & Wiener, 1945)**

** At the time they weren't talking about the bond.*

N.B. The cover image is created from the output of the SafetyNet model. All images of graphs in this project were generated using the model.

Glossary

Terms

Term	*Definition*
Adverse Selection	A situation in which less desirable outcomes are more likely to occur.
Deductible *(see Excess)*	A surcharge payable when making a claim against insurance. The effect is to set a floor for the pre-charge size of claim. Also referred to in as Excess (in the UK).
Demand-side	Entities that provide demand for a good or service (in this case the Insured).
Excess	*See Deductible*
Indemnity	Insurance cover compensates the insured for loss or damage but doesn't permit the insured to make a profit.
Insurable Interest	The insured must suffer a loss if the item insured is lost or damaged.
Insured	The entity purchasing the insurance policy.
Insurer	The entity issuing the insurance policy.
Moral Hazard	A situation in which one party gets involved in a risky event knowing it is protected from downside risk at the expense of another party. This arises from one or both parties having incomplete information.
Reinsurer	An entity that insures the risks of other insurers.
Retrocessionaire	An organisation that reinsures Reinsurers.
Risk of Ruin	The probability that losses from accepting a risk exceed available capital held.
Safety Capital	Capital held by an investor in excess of revenues to achieve a desired Risk of Ruin.
Safety Loading	Uplift to a premium applied by an Insurer, in excess of the base cost, to protect against higher claims than expected.
Supply-side	Entities that provide the supply for a good or service, in this case Insurers.

Abbreviations

Acronym	*Expansion*	*Meaning*
CAGR	Compound Annual Growth Rate	Geometric progression ratio that provides a constant growth rate over a period of years.
ILS	Insurance Linked Securities	Financial instruments sold to investors, backed by insurance assets. The value is therefore determined by insured loss events of the underlying asset.
MCR	Minimum Capital Requirement	A hard floor threshold of capital an Insurer must hold to cover claimed losses, in accordance with the EU Solvency II Directive.
RTO	Recovery Time Objective	Time objective within which full recovery of a system's functionality is expected.
SCR	Solvency Capital Requirement	A soft floor threshold of capital an Insurer must hold to cover claimed losses, in accordance with the EU Solvency II Directive.
SPV	Special Purpose Vehicle	An entity established to hold assets and isolate them from a parent organisation in case of, for example, bankruptcy.

1 Executive Summary

When addressing risk in Information Security one option is to transfer it, an example of which is the growing industry of Cyber Insurance. This risk transfer not only offers a valuable service to organisations with exposure to Information Security risks, but also can function as a bridge to capital markets.

This project will introduce cyber insurance as well as Credit Ratings, an existing bridge between an organisation and investors in the capital markets. It will then look at recent Cyber Insurance literature in more depth, particularly in relation to modelling approaches used, before introducing a cyber insurance model for further analysis.

The model will use a graph to represent individual systems on a network, which in turn incur costs due to incidents that compromise their Information Security. Compromise of these nodes may arise through different mechanisms and result in impacts based on available empirical statistics, leading to losses which may be covered through insurance.

The risk these profiles then transfer onto the Insurer will then be considered, including the application of Catastrophe Bonds, or Cat Bonds, for managing tail-risk, as well as how Credit Ratings may help in this regard going forward.

2 Introduction

Awareness of Information Security has become increasingly prevalent in recent years with high profile incidents making headlines. NotPetya, for example, was expected to "impact [Maersk's] results negatively by 200-300m USD" (Maersk, 2017). Direct costs may be surpassed by the less quantifiable potential for reputational damage. This combination of awareness and potential impact is likely to drive increased cyber security investment.

As well as investment in controls, organisations may also choose to share risk in order to achieve their desired risk tolerance. Cyber insurance offers one such risk-sharing mechanism, though it is still widely perceived to be early in its lifecycle. Growth has been slower than expected due to several contributory factors, including a lack of information, a rapidly changing threat landscape and accumulation risk to insurers (Fahrenwaldt, Weber, & Weske, 2018).

Due to idiosyncrasies of Information Security, a Cyber Insurer may accumulate risk much faster than would occur in other insurance markets. Where those segments can often rely on independence of outcomes, this diversification is not so dependable where Information Security comes into play. For example, a vehicle or industrial accident in the UK is likely to be unrelated to similar events in Brazil, Saudi Arabia or Japan, but as WannaCry[1] demonstrated this is not true for malware.

Beyond the above instances of malware, hacking incidents demonstrate how credit and cyber risk may be closely tied. AMCA was recently forced to file for Chapter 11 bankruptcy protection (Kovacs, 2019) due to the costs incurred following its breach by the Magecart hacking group.

But while this demonstrates the damaging connection between cyber and credit, a beneficial link may exist in the form of Credit Ratings. Derek Vedala, Moody's newly appointed head of Cyber Risk is reported to have said they're planning on incorporating cyber risk into existing Credit Ratings, prior to considering a standalone rating (Fazzini, 2018). With the transition to inclusion of cyber risk in ratings comes the opportunity for insurers to gain another data point in the estimation of cyber risk posed by some companies.

Firms that see their rating change will experience an indirect incentive to invest in Information Security, as their worsened Credit Rating leads to higher borrowing costs and increased Cost of Capital. This indirect cost may be complemented by proposed indirect benefits such as tax deductibility of Information Security investment, a move that has already been proposed to the UK government by the ICAEW accounting body (ICAEW, 2019).

These incentives could all contribute to the growth of the Cyber Insurance sector forecast by a variety of sources from academia and industry. In spite of the wide range of outcomes shown in Figure 2-1, estimates for the size of the global insurance market, either interpreted or explicitly stated as total written insurance premiums consistently exceed a double-digit Compound Annual Growth Rate (*CAGR*). Data from 2017 even suggests that the scale of the industry beat forecasts, despite a historical tendency for the sector to underperform (Eling & Zhu, 2018).

[1] WannaCry victims included the NHS in the UK, Petrobras in Brazil, Saudi Telecom Company in Saudi Arabia and Honda in Japan. This demonstrates the cross-sector nature of cyber incidents too.

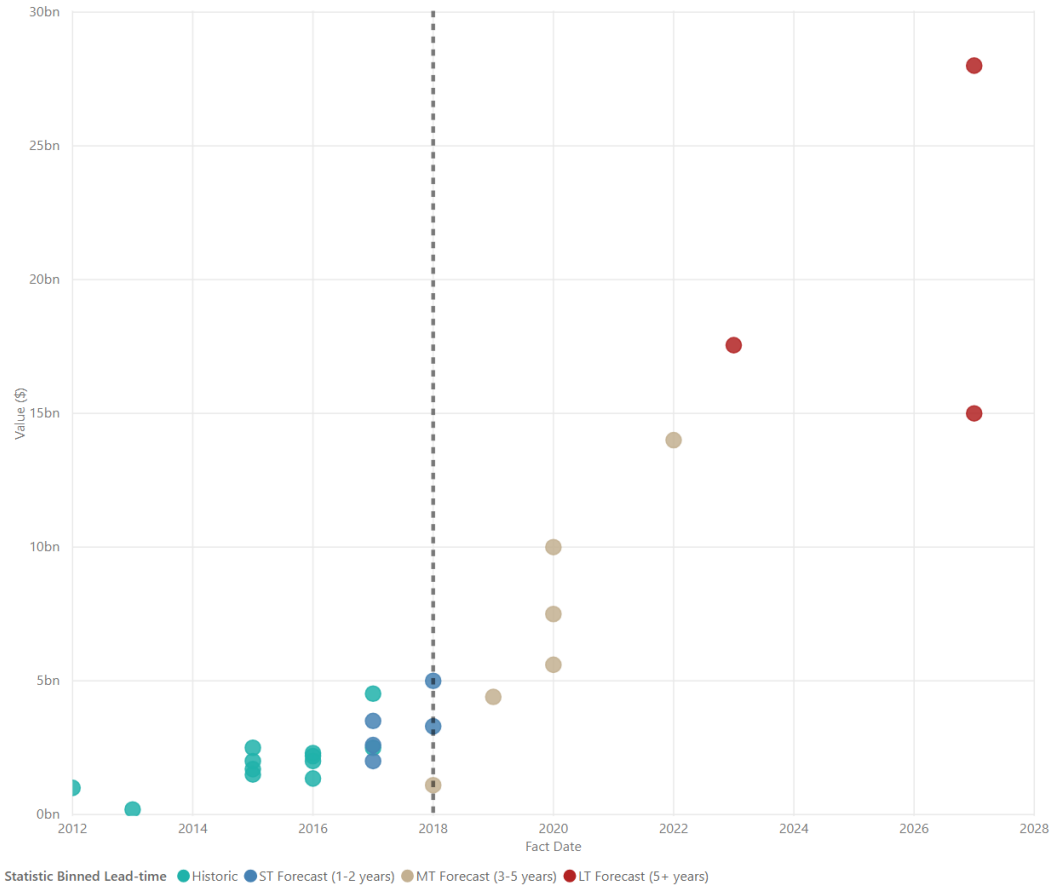


Figure 2-1 - Published Estimates for Global Cyber Insurance Industry Size. Data represents full-year estimates, so 2017 historic data reflects the total to EOY 2017, produced in mid-2018. Colouration indicates the difference between the date the forecast was made and the period the forecast was of. Dotted line reflects the most recent period in which actual figures can exist. Full source listing is provided in Appendix 10.1

There is clearly growth expected in Cyber Insurance even in the lower growth forecasts, but with this potential reward come risks. As highlighted by (Artemis, 2016), insurers may need to resort to reinsurance or securitisation (referred to as Insurance Linked Securities, or *ILS*) to handle these risks, or fall afoul of the risks themselves (Fitch Ratings, 2016). This paper aims to shed some light on the risk that insurers may face.

3 Background

Some topics covered by this document are in disciplines that rarely intersect. Therefore, this section will provide both an introduction to concepts used in this paper as well as provide an overview of the recent literature for the topic.

3.1 General Insurance

Insurance and the wider insurance industry have been around for centuries, with the first mention of Lloyds as a broking location in 1688 (Lloyd's, 2018). Consequently, there is a wealth of literature on conventional insurance practices and what follows is a summary of important concepts for use in this paper, from the perspective of the Insured (purchaser of the insurance policy) and the Insurer (provider of the policy).

While nuances of Cyber Insurance undoubtedly still exist, these high-level concepts still apply.

3.1.1 The Insured's Perspective

The Insured's perspective is a natural starting point as it is likely to be the side most widely experienced, especially at the retail level. One approach is through the consideration of the "6 Cs"; Cost, Coverage, Capacity, Capabilities, Claims and Compliance (Hopkin, 2017).

Cost typically falls into two categories. The first is the fixed periodic payment required to obtain the policy, referred to as the premium. The second is a threshold the insured must meet prior to receiving any compensation in the event of a claim, illustrated in Figure 3-1.

Coverage determines the limitations and exclusions of the policy. This extends to both the assets covered by the policy and the events that may threaten these assets.

Capacity is a significant consideration for very large insureds and relates to capability of the insurer to cover any events that may arise. If the insured is too large, a single insurer may be unable to cover losses. This may be resolved, either by the insured through spreading risk across multiple insurers and policies, or by the insurer through syndication (forming a group with other insurers) or reinsurance.

Capability relates to services an insurer may be able to offer beyond financial insurance itself. This may include consultancy, planning, and forensic services. A comprehensive single-point Incident Response, sometimes called a "breach coach" has been highlighted as an important part of the insurance offering (Bittner & Harvey, 2019).

Claims includes the handling of any loss event, clearly defining the coverage and responsibility for determining restitution actions and payments. Often, insurance in isolation is insufficient, with the insured having to implement a level of business continuity planning in order to acquire the policy.

Compliance includes legal considerations arising from the acquisition of an insurance policy and may be internal to the policy itself, or external requirements placed on the insured by law. Internal requirements may include contract exchange prior to commencement of the policy period, providing contract certainty. External requirements include legal requirements for holding insurance, or tax obligations such as Insurance Premium Taxes.

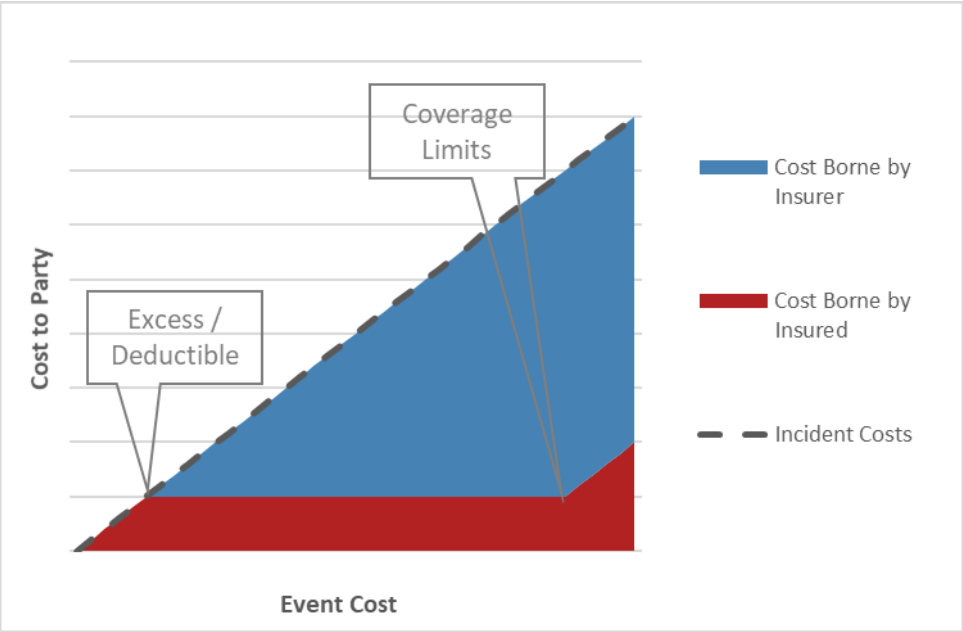


Figure 3-1 - Cost Obligations by Party for an Insured Event

Figure 3-1 shows an idealised division of costs to illustrate the effect of several key insurance terms. The first is the *Excess* or *Deductible*, which is an agreed threshold beneath which the Insured is liable for costs and above which the Insurer is liable for the increment. By accepting these limits an Insured can benefit from reduced premiums, while for the Insurer it serves as a risk limitation device and can ensure they must only deal with sufficiently material events. The term "Excess" is predominantly used in the UK, while "Deductible" is used in the US.

Coverage Limits arise when the Incident Costs exceed the terms of the policy. This may be quantitative, where costs exceed a numerical threshold and are no longer covered, or qualitative whereby claimed costs are not eligible due to their intrinsic properties in relation to the policy contract. As with an Excess, Cover Limits offer the Insured an opportunity to reduce their premium costs, while the Insurer can benefit from limiting their maximum liability.

There is a potential source for confusion between UK and US terminology as alluded to previously. While the term "Excess" relates to the lower limit mentioned previously, in the US "Excess Insurance" refers to a supplementary policy held in addition to the base coverage in order to provide an increased Coverage Limit.

The above example graph assumes perfect insurance, with all insured costs borne according to the prescribed balance. This may of course be a stretch from the uncertainty of reality, but gives rise to an important principle of *Indemnity*, in which the resolution should be neither a punishment nor a source of profit to either party.

3.1.2 The Insurer's Perspective

The premise for all these forms of insurance is the same, with the Insurer offering to bear some or all costs incurred by any event covered by the policy. An Insurer would however be offering this service to a portfolio of clients and therefore views risk in a probabilistic fashion as the likelihood of all Insureds making claims simultaneously is typically slim. An example of this is shown in Figure 3-2.

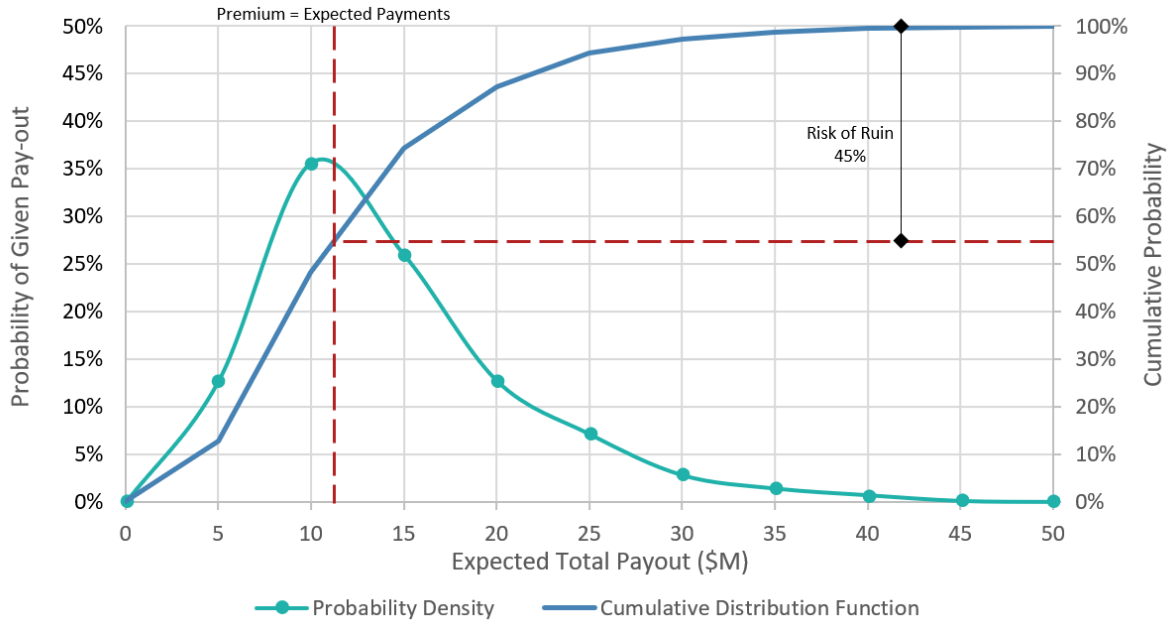


Figure 3-2 - Example Expected Insurance Claim. Assumes 70 identical Insureds, each with the same claim properties.

In the example above, the average (or Expected) claim is $12M. Under the Net Premium Principle, in which the premium should equal the expected claim, each Insured would pay a premium equivalent to their individual Expected Loss. On average, this will result in receipts equalling claims and the Insurer breaking even (ignoring extraneous costs such as administration).

Such a strategy does however result in an excessively high *Risk of Ruin*, with a 45% likelihood in the example above that the Insurer will be required to pay more than they have received in premia. Therefore, alternative approaches such as the Standard Deviation or Equivalent Utility Premium Principles exist which adjust the premium upward in accordance with the corresponding metric, thus reducing the Risk of Ruin to the Insurer. This uplift to the premium is referred to as *Safety Loading*.

The approach used for analysis later will be the Standard Deviation Premium Principle, in part due to the relative simplicity but also its' wide applicability. The formula, below, shows that the premium ($H(x)$) is the sum of the Expected Loss ($\mathbb{E}[x]$) plus a safety-loading multiple (λ) of the variance ($\sqrt{Var(X)}$).

$$H(x) = \mathbb{E}[x] + \lambda\sqrt{Var(X)}$$

Equation 1 – Standard Deviation Premium calculation (Xu & Hua, 2017)

Contrast this with an alternative such as Equivalent Utility, which incorporates idiosyncrasies of the Insurer and is shown below. In this case the aim is to ensure that the utility from a given initial wealth ($u(\omega)$) remains the same as the expected outcome from that same wealth, minus claims (X), plus the premium received ($H(x)$). As the utility function differs from one Insurer to the next, so will the outcome from such an equation.

$$u(\omega) = \mathbb{E}\big[u\big(\omega - X + H(x)\big)\big]$$

Equation 2 - Expected Utility Premium calculation (Xu & Hua, 2017)

As well as raising in-period premiums, Insurers also buffer their risk by retaining capital from previous periods or holding equity from investors, which may be used in the event of higher-than-expected claims. Minimum capital requirements are often mandated, with the UK and other European countries bound by Solvency II in the form of the Solvency Capital Requirement (SCR) and Minimum Capital Requirement (MCR).

The SCR is set at a 99.5% confidence interval and is considered a "soft" floor, while the MCR is set at a lower level of 85%, but is a "hard" floor, below which the national regulatory body would be expected to intervene (Insitute and Faculty of Actuaries, 2016). The approaches for calculation, as well as quality of asset composition, vary between the two measures but this will not be addressed here.

These risks and requirements culminate in a much more complicated insurance marketplace than a simple bilateral relationship between Insureds and Insurers. An Insured may choose (or be required) to offset their exposure through several insurance intermediaries, summarised in Figure 3-3.

Self-insurance, Captive-insurance and Insurer-based approaches differ primarily in terms of beneficiaries and capacity. Self-insured companies will pay their premiums to an associated entity that only they use, which in the absence of claims will result in increasing assets. The company may benefit if there is no requirement to claim but may suffer from increased exposure and potentially limited capacity if a large claim is necessary[2].

Captive Insurance occurs when a group of companies, usually with similar exposure, form a common entity to aggregate insurance claims. The benefits are less directly attributable than in the case of self-insurance, but the aggregation allows for greater depth of cover in the event of a claim.

The typical insurance model is for a third-party Insurer to take the risk, potentially via an Insurance Broker who mediates the market between Insured and Insurer. In this case, benefits from a lower claims history than expected remain with the Insurer but the Insured does have the greatest insulation from loss in the event of an incident, provided it is within coverage limits.

All three approaches may then choose to offset risk with a Reinsurer, who essentially insures the Insurers against losses that exceed their risk tolerance. Furthermore, a Retrocessionaire provides the same function but at one level higher, insuring a Reinsurer against their Risk of Ruin.

[2] (Brealey, Myers, & Allen, 2011) perform a Case Study on the Self-Insurance policy of BP, intriguingly written prior to the blow-out of Macondo in 2010.

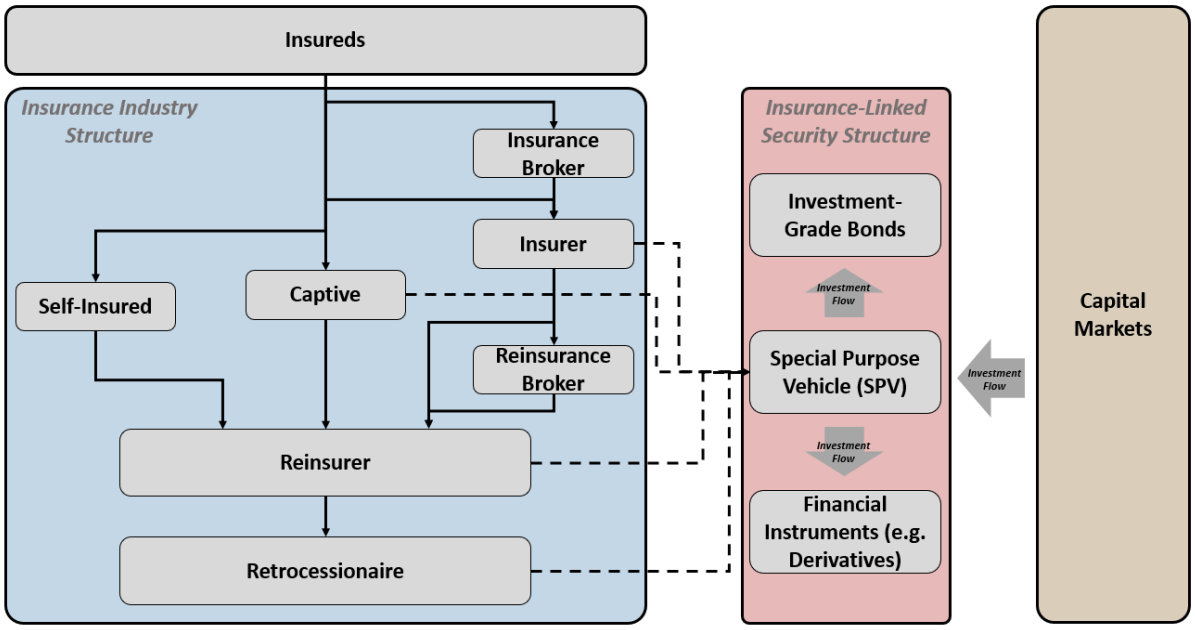


Figure 3-3 - Insurance Industry and Insurance-Linked Security Structure, based on (Payne, 2017) and (Fenn & Cid, 2017)

The ILS provides a means for insuring entities to pool risks with others in the Insurance Industry as well as access sources of finance from the wider Capital Markets. Through this securitisation process, insurance liabilities are moved into an SPV along with assets to back those liabilities (typically low-risk bonds). Investors may then choose to invest in this SPV, benefitting from the income generated by premium payments but at the risk of losing a proportion of their investment if the insurance policies on which these premiums are paid claim enough to consume the capital of the SPV.

Catastrophe, or Cat Bonds, are a special case of this security. As with other ILS's, the SPV holds the liabilities and backing assets and the investor receives income from the premium payments, but in this a "trigger event" causes the payment of the collateral to the insurance policyholders. In the case of natural disasters such as hurricanes, this is a prescribed measurable event such as the wind speed at a specified, ideally insusceptible, location in proximity to the insured.

3.2 Cyber Insurance

Cyber Insurance is still considered to be "in its infancy" (Aon Inpoint, 2017) from a market maturity perspective, although some literature would suggest otherwise[3]. This section will look in more depth at the material that has been published to date in this nascent sector.

Market research of the sector by (ENISA, 2016) suggests demand is impaired by a lack of understanding of both the application process and coverage itself. This lack of understanding may give rise to some of the complications detailed later. Progress is however being made in extending supply of cyber insurance beyond the enterprise (Marvin, 2018), with retail insurers beginning to extend their policies to cover cyber incidents for individuals (Little, 2019).

When understanding insurance risks, a longstanding framework by (Berliner, 1985) has more recently been applied to Cyber Insurance. Based on nine categories of importance to the Insurer, this has been adopted as an underpinning for both technical papers and informative articles.

	Insurability Criteria	Risk Type
1	Insurance Cover Limits	Market
2	Insurance Premium magnitude	Market
3	Information Asymmetry (Moral Hazard & Adverse Selection)	Actuarial
4	Randomness of Loss Occurrence	Actuarial
5	Average Loss per Occurrence	Actuarial
6	Average Frequency of Occurrence	Actuarial
7	Maximum Possible Loss	Actuarial
8	Public Policy	Societal
9	Legal Restrictions	Societal

Figure 3-4 - Insurability Limits Framework by (Berliner, 1985)

While this section will provide an overview of the current state of Cyber Insurance, a comprehensive report by (Payne, 2017) looks at the difficulties faced by insurance counterparties in significant detail, focussing primarily on commercial and legal issues.

3.2.1 The Insured's Perspective

Commercial and legal aspects of Cyber Insurance are particularly challenging as they give rise to exceptions that are uncovered by an insurance policy, referred to as Cover Limits. A recent report by (Mactavish, 2018) found that, of the eight main issues cited by Insureds, the top 6 related directly to these Cover Limits while the remaining two were problems the Insured expected would arise in the event of a claim.

Such Cover Limits are a necessary mitigation on the part of the Insurer, as they can help protect from Moral Hazard by the Insured, who may otherwise perceive their insurance policy as a reason to increase their risk exposure. Research by (ENISA, 2016) suggests such risk-seeking behaviour may even arise unintentionally, with some 40% of respondents claiming they didn't understand their own exposures. This in turn makes the task for an Insurer to understand their exposure even trickier.

[3] (Ogut, Menon, & Raghunathan, 2005) state that "The conventional wisdom that firms are reluctant to buy cyber insurance because [sic] insurance market is immature is not correct". With the benefit of hindsight, the market growth in the intervening period suggests otherwise. This doesn't necessarily invalidate their underlying finding that interdependent risks reduce incentives to invest.

An alternative mitigation for Moral Hazard proposed by (Pal, Golubchik, & Psounis, 2011) is “Aegis”, essentially a pure risk-sharing policy. Instead of a typical deductible structure, which places all liability of small losses on the insured and a very high proportion of major losses on the insurer, this proposal pro-rates costs between insurer and insured ensuring both parties are liable for any losses. The game-theoretic outcome of this research suggests this structure would increase insurance desirability, but this does come with a cost. As both parties are vested in any restitution, decisions regarding course of action may become more difficult to achieve.

This form of risk-sharing may also be an interesting addition to the “Cyber Risk Analysis and Modelling” (“CRAM”) framework proposed by (Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2017), which offers a decision-making approach for Insureds, based on likelihood and impact to determine whether to implement controls, externally insure or self-insure. The conclusion, that external insurance be used for low frequency and severity events while self-insurance is used for high severity and low frequency events, is counterintuitive, particularly given the rationale that it is “preferred to ensure loss protection by reducing the size of the loss”. Self-insurance still places the entire liability with the insured, only affecting the timing and preparedness rather than reducing it.

3.2.2 The Insurer’s Perspective

(Johnson, Böhme, & Grossklags, Security Games with Market Insurance, 2011) suggest cyber insurance concerns arose in two distinct phases, though literature would suggest that these phases are substantially intertwined. The first phase concerned the lack of actuarial data, while the second extended to cover Randomness (or more precisely a lack of randomness due to interdependence), Information Asymmetry and Cover Limits.

While these three categories shall be used to structure the literature below, research in the field continues to be hampered by a lack of data highlighted in the first phase and contributed to by the dynamic landscape of information security. Further phases may consider other categories of the Berliner framework going forward as work by (Beiner, Eling, & Wirfs, 2015) has shown much of it to be directly applicable.

The problem of Randomness was researched by (Böhme, 2005) who, due to a lack of data, relied on a homogenous portfolio and binomial distributions to determine the impact of interdependence. The findings suggested Insurers may achieve greater resilience when covering fewer, larger policies than when exposed to a multitude of smaller yet unexpectedly correlated ones. This finding is a noteworthy reminder that diversification is simply unachievable regardless of the number of holdings if they are correlated.

Unfortunately this preference for fewer, larger policies would conflict with more recent research by (Tondel, Seehusen, Gjaere, & Moe, 2016), who looked at the continued discrepancy between expected and actual breach costs. Despite the persistent lack of data, they suggest two approaches to help insurers mitigate the issue. First, a large customer base may help build datasets and improve sales process efficiency. Second, Insurers should evaluate potential customers using questionnaires, scrutinising high-risk clients which are identified using size or insured value as risk proxies given the lack of data.

Information asymmetry was considered by (Schwartz, Shetty, & Walrand, 2010), who looked at two ways in which Insureds may abuse this asymmetry in order to disproportionately benefit from their insurance policies. The first is a pre-meditated disclosure of subtly incorrect information to acquire a policy at a lower premium, while the second is through providing correct information that may then diverge due to Moral Hazard. Since both are premised on the ability of a malicious Insured to subvert contractual safeguards, this leads to the claim that growth will be impeded where the prevalence of malicious actors (and the ability to detect them) is limited, with the market for Internet risk management specifically singled out.

Frameworks to help address information asymmetry already exist, such as a risk schema by (Cambridge Centre for Risk Studies, 2016), or are about to be published as a forthcoming ISO 27102 standard (ISO, 2018). While they may help reduce the information gap between Insurer and Insured at the time of entering the policy, avoidance of subsequent risk seeking behaviour due to Moral Hazard can only be addressed through the Cover Limits.

Cover Limits were the focus of (Romanosky, Ablon, Kuehn, & Jones, 2017), who looked at them from a commercial perspective by comparing policy wording to evaluate the level of similarity. They find that policies from different providers were more consistent than expected, though this was offset by a wide variety of exclusions[4] which may have a significant effect on the Insured's coverage. Mobile devices and IoT were also highlighted as a grey area, with no explicit coverage.

While distinct categories in the Berliner framework, the boundaries imposed by Cover Limits are implicitly connected to the setting of premiums. The latter has been the subject of qualitative research by (Romanosky, Ablon, Kuehn, & Jones, 2017), who suggest the level of rigour on policy pricing may be done to varying degrees of rigour in practice. They found underlying pricing mechanisms were based on one of three approaches. The simplest was a simple base rate, followed by a "base rate with modifications", using readily available business properties to determine adjustment factors. Thirdly, "Information Security Pricing" was the most complex, incorporating information security posture properties acquired through questionnaires. Insurers were understandably reluctant to divulge detailed information, but the more detailed approaches imply quantitative methods have been performed to determine the appropriate adjustment factors.

Quantitative analysis by (Tondel, Seehusen, Gjaere, & Moe, 2016) shows that the premium-to-cover limit of cyber insurance is typically three times higher than established general liability and six times higher than property insurance. This means that for a given premium the cover is lower than it could be, which offers further substance to the message conveyed in a PWC report (PWC, 2015) that large companies were having trouble acquiring the level of cover they desired.

A mitigation for these higher premiums is that Information Security incidents may not always be a negative outcome for the organisation. While insurance would still cover eligible costs, (Spanos & Angelis, 2016) showed in their extensive literature review that while resulting stock market movements were predominantly negative, some showed statistically significant positive outcomes. Such findings are consistent with those of (Dubner, 2018) who showed that a good apology can

[4] Among the top 10 exclusions that may be particularly concerning in cyber security are:
#2 – Negligent disregard for computer security (may be triggered by poor password practices e.g. defaults)
#3 – Loss to system not owned or operated (e.g. supply chains)
#6 – Act of terrorism, war, military action (one current example is the ongoing Mondelez vs. Zurich litigation)

increase market cap, suggesting that investors' expectations can counterintuitively improve as a result of the breach.

While there may be scope for these costs to fall in the future, which would undoubtedly be welcomed by Insureds, this may also be a symptom of the increased risk faced by Insurers. This hypothesis was extended by (Eling & Zhu, 2018) who examined the relationship between Insurers offering cyber insurance and their size, risk tolerance, corporate structure and existing diversification. While they did find statistically significant correlations, the research did not seem to adjust for the potential third-cause fallacy – that these correlations exist simply because of one root cause, scale.

Finally, it's worth noting that Catastrophe modelling in context of cyber security remains a largely understudied area. Non-cyber methods rely on extensive real-world (such as meteorological or geological) data for regression analysis (RMS, 2008), an option which is not available for cyber insurance, as highlighted earlier. A collaboration of AIR, BitSight Technologies and Risk Based Security was reportedly working on a Cyber Catastrophe model as early as 2015 (Beckett & Booth, 2015), but no further details of this work have emerged. Work by (Fenn & Cid, 2017) on the area remains unpublished.

3.2.3 Beyond the Insured and Insurer – Externalities of (Cyber) Insurance

Thus far the benefits and risks to Insurer and Insured have been discussed, but there is a strong case for both cyber security and insurance to be considered a public good.

In a paper by (Johnson, Böhme, & Grossklags, Security Games with Market Insurance, 2011), a Game Theory model was used to show how cyber security investment benefits not just the investor but also the wider technology ecosystem by cutting down on infection vectors. They also find that cyber insurance is complementary to partial protection mechanisms, only substituting for the high cost (and low capital efficiency) investments.

These positive externalities are also identified and extended by (Beiner, Eling, & Wirfs, 2015) who find that the act of preparing to insure also forces a company to take stock of their cyber security situation, an activity which they may otherwise have neglected.

While this is good news for the industry, (Böhme, 2005) raises the possibility that challenges posed by interdependence may diminish some of the benefits typically arising from insurance. In a fully functional insurance market, Insurers have an incentive to develop solutions to issues that no single Insured in isolation may see a need for, which in turn would not only directly reduce claims, but may also benefit other uninsured parties. However, as the paper suggests that Insurers would be less inclined to cover smaller policies, the insurance market would be stunted in terms of liquidity and depth, reducing Insurer's impetus to drive research and provide these benefits.

3.3 Credit Ratings

Credit Ratings rose to prominence during the Financial Crisis and the academic literature since has remained focussed on this event. To date the intersection with Information Security remains a blind spot, despite ominous warnings by businesses such as (Capco, 2018) that this may be the root cause of the next crisis.

Credit Ratings themselves are an ordinal scale representing the estimated likelihood of default and are typically applied to companies and sovereign states. Individual ratings also exist and, while the principle of estimating creditworthiness remains the same, the approach and scale differs. Ratings may also be applied to specific financial products, such as corporate debt issuances and Special Purpose Vehicles (SPVs) created to isolate, securitise and protect assets from a Parent, such as those that must be held by an Insurer in order to back a policy (as mentioned in Section 3.1.2).

At the Sovereign and Corporate scale, Credit Ratings are primarily offered by the "Big 3" ratings agencies of Moody's, Standard & Poors and Fitch. Each agency may maintain their own outlook for the same target but, while their scale nomenclature may differ, they consistently map according to regulations by the (European Banking Authority, 2019) and shown in Figure 3-5.

	Expected Default Rate Range						
Credit Quality Step	**Lower**	**Mid**	**Upper**	**Fitch**	**Moody's**	**S&P**	**Description**
1	0%	0.10%	0.16%	AAA AA+ AA AA-	Aaa Aa1 Aa2 Aa3	AAA AA+ AA AA-	Prime High grade
2	0.17%	0.25%	0.54%	A+ A A-	A1 A2 A3	A+ A A-	Upper medium grade
3	0.55%	1%	2.39%	BBB+ BBB BBB-	Baa1 Baa2 Baa3	BBB+ BBB BBB-	Lower medium grade
4	2.40%	7.50%	10.99%	BB+ BB BB-	Ba1 Ba2 Ba3	BB+ BB BB-	Non-investment grade speculative
5	11%	20%	26.49%	B+ B B-	B1 B2 B3	B+ B B-	Highly speculative
6	26.50%	34%	100%	CCC+ CCC CCC- CC C	Caa1 Caa2 Caa3 Ca C	CCC+ CCC CCC- CC C	Substantial risks Extremely speculative Default imminent
				DDD DD D	- - -	RD SD D	In default

Figure 3-5 - EBA Expected Default Rate and Alignment of Credit Ratings between the "Big 3" (EU, 2016)

While this table is important for aligning the ratings of the agencies, it is important to bear in mind that Expected Default Rates are not only forecasts but also momentary snapshots prone to subsequent change. Analysis by S&P into the subsequent default performance of rated companies, shown in Figure 3-6, shows a couple of important insights.

The expected midpoint default rate (dashed line) of a given band is consistently significantly lower than the actual default rate of the rating band. The magnitude of this difference is greater than statistical differences would allow, such as differences between mean and median, or population sizes, implying that actual default rates are significantly higher than expected. This difference arises over even relatively short timeframes, especially for the less creditworthy ratings.

For stronger ratings, this difference is less visible though arguably just as stark, with AA/AAA ratings expecting default rates of at most 0.16%, yet actual figures show default rates at over 1% on a 20-year time horizon. Crucially, the order of expected and actual default rates remains in sequence, maintaining their ordinality.

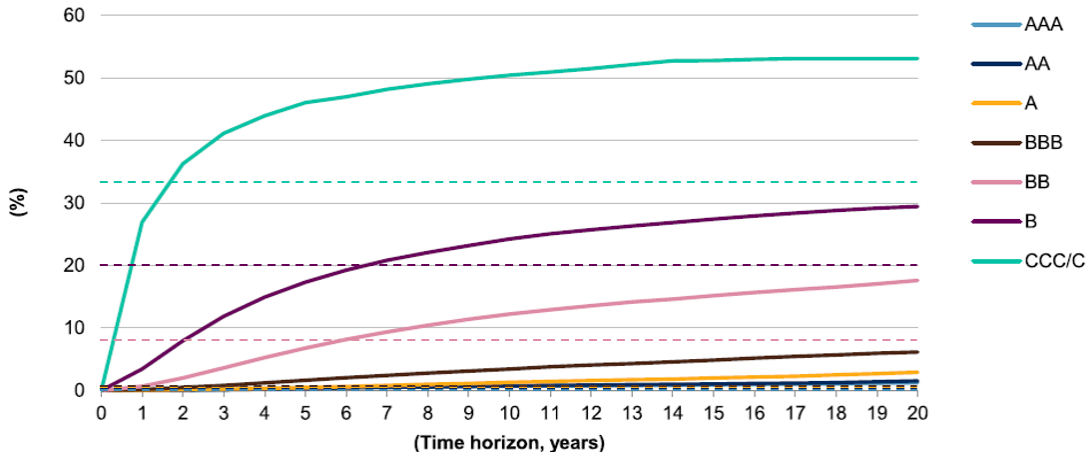


Figure 3-6 - Historical Default rates of Rated Companies Over Time. Dashed lines indicate expected mid-point default rate. Y-axis shows proportion of rated companies that default in the timeframe. Source: (Standard & Poors, 2019).

This highlights an important point; a credit rating is not only a forecast prone to errors, but it can be revised. Ratings Agencies therefore also publish another important piece of information referred to as the outlook. This may be positive, negative or neutral, indicating the direction the agency anticipates the credit rating may move as a result of foreseeable but uncertain events.

Announcements by the Big Three have shown that cyber security is a growing consideration in their activities, with (Williams, Schulz, Tesher, & Hazell, 2015) at Standard & Poors analysing cyber risks by industry in 2015. S&P have since followed this up with a statement that their Global Ratings360 service will include insights from Guidewire Cyence (S&P Global, 2018).

In 2017, (Fitch Ratings, 2017) released a statement highlighting their growing concern regarding cyber risk to Financial Institutions. Later that year they went on to highlight the potential of the cyber insurance market, noting the growing risks to companies and insurers (Fitch Ratings, 2017), though it maintained a "neutral" stance on insurers in spite of its prior warnings.

The most interesting comments regarding Ratings and Cyber risk were made by Moody's newly appointed head of Cyber Risk, Derek Vadala, who's reported (Fazzini, 2018) to have said they're planning on incorporating cyber risk into existing credit ratings prior to considering a standalone rating. The company had previously stated cyber risks may catalyse stress-test scenarios for rated companies, albeit with a high likelihood of government intervention for power & utilities companies in particular (Moody's, 2018).

While niche players already offer Cyber Ratings and purportedly offer great benefits to the insurance industry among others, these claims should be approached with caution. Material typically originates from the company in question or is produced by vested third parties such as consultancies, so facts are likely to be embellished and biased.

Some offerings, such as Guidewire Cyence seek to address Insurer's lack of actuarial data through Big Data analytics (Guidewire, 2018). Conversely, providers such as FICO (FICO, 2018), UpGuard

(UpGuard, 2018) and BitSight (BitSight, 2018) cater to the Insured, using structures very similar to consumer credit scores. Based on the available information and volume of sites they monitor (UpGuard, 2019), such approaches are likely based upon known vulnerability scanners and may therefore see success in identifying basic red flags, but struggle when faced with Advanced Persistent Threats (APT), Insider or other such pernicious threats.

While Insurers are among the user cases for such tools, the current users are more likely to be businesses seeking a commercial edge and insight into how outsiders (including their Insurers) perceive their cyber security posture (EuroFinance, 2017). They may also be used to supplement assessments of counterparty risk, such as supply chain, customers, M&A activity or future business partners (Olyaei, Ambrose, & Wheatman, 2018).

Despite the fate of AMCA, mentioned earlier, to date the first and only instance of Information Security events impacting a Credit Rating is Equifax (Fazzini, 2019), a company that coincidentally provides consumer credit scores. The repercussions of a large-scale breach of customer data in 2017 continue to be felt to this day, with attrition of over half of board positions and total Information Security costs since the incident claimed to reach $1.35bn by Q1 2019 (Equifax, 2019, p. 26), though these costs are covered more detail in Appendix 10.6. This disruption has caused the Ratings Agencies to revise their forecasts and not only reduce the rating by a notch, but also maintain a Negative outlook in case further downgrades are necessary.

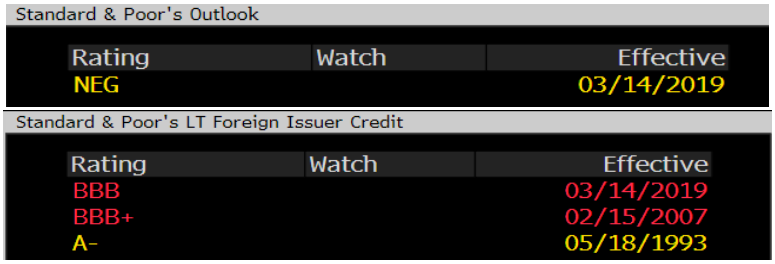


Figure 3-7 - Current Credit Outlook and Ratings Change History from (Bloomberg, 2019)

Isolating the impact of this Credit Rating change is difficult as many factors influence Cost of Capital (particularly Debt) and such impacts would typically only affect newly issued capital[5]. However, there are two ways of looking at this. The first is through Equifax' own debt issuance, though attribution is difficult. The second is through aggregate data of Ratings and Credit Spreads.

Equifax happens to have issued debt twice since 2016 – once pricing on 05/05/2016 and again on 23/05/2018 (Bloomberg, 2019), so the two issuances straddle the occurrence and announcement of the breach, although both predate the ratings downgrades. In both instances the debt was Callable with 5-year maturity and the underlying debt market was rising with further rises expected, although the magnitude of the bond fell from $500M to $400M and the issuance.

[5] Debt (Bonds) and Equity (Shares) already in the market may gain and lose value in the secondary market and lead to difficult questions from investors, but don't directly impact the company's cash position.

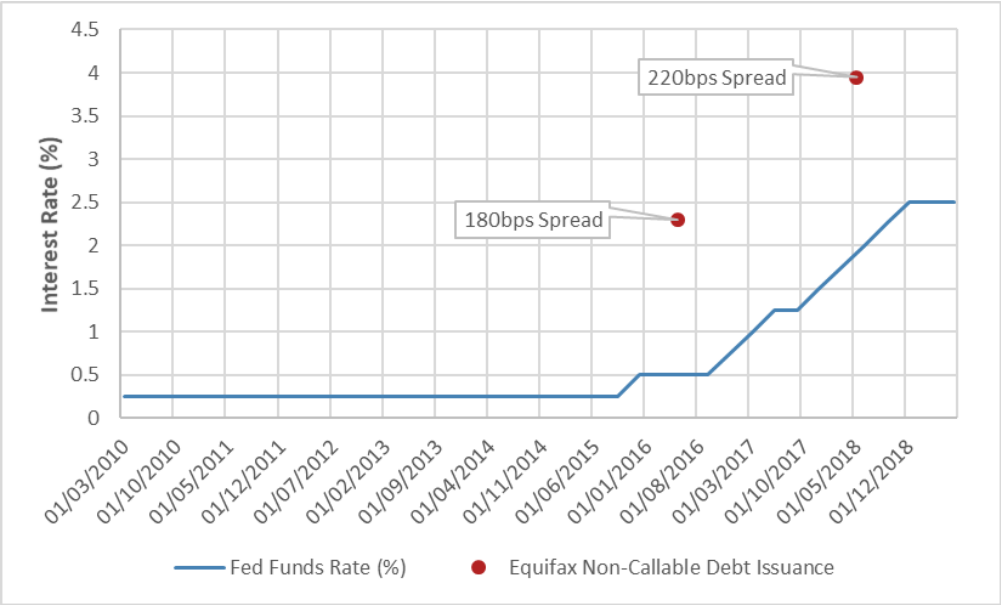


Figure 3-8 - Fed Funds Rate compared to two Equifax debt issuances. Data from the Federal Reserve and Bloomberg

Changing circumstances make it impossible to attribute this change directly to the breach, but if this is the case then a 40bps rise is quantifiable. This increase of 40bps on the $400M bond equates to increased interest payments by $1.6M per year over the bond's lifetime. If this downgrade becomes permanent and Equifax must cycle debt at this slightly increased rate, interest payments on the entire $2.65bn outstanding would be $10.6M higher than if they hadn't been breached.

A generalised alternative to this circumstantial approach is to use aggregate Ratings vs. Credit Spread data, provided by the Ratings Agencies themselves.

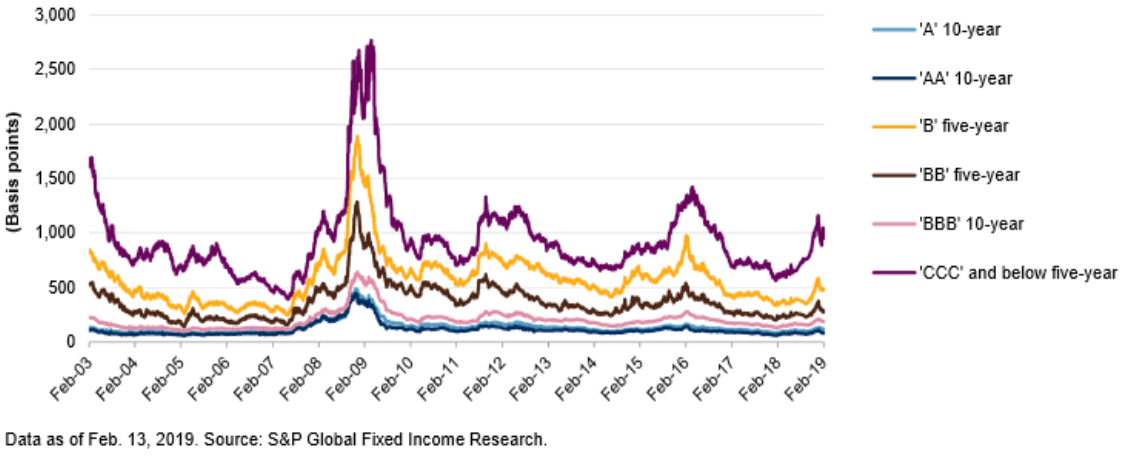


Figure 3-9 - Credit Rating vs Credit Spread, measured in Basis Points (Vazza, Kraemer, & Gurwitz, 2019)

Figure 3-9 shows the average spread from the base rate for all companies of a given credit rating. If Equifax were to suffer further downgrades and transition from the 'BBB' line to the 'BB' line, this is currently around 100bps. Fortunately, this appears to be in line with the apparent 40bps increase from 'BBB+' to 'BBB'.

The transition between absolute static numbers such as outstanding debt, and periodic cash flows such as revenue will prove important going forward. For a specific target organisation, such as

Equifax, implications of Credit Ratings on periodic cash flows may be determined easily from numbers provided in Financial Statements and present in any listed company's Annual Report. A direct calculation may be done by dividing revenue (Income Statement) with the appropriate debt figure (Balance Sheet). Revenue is generated over the course of the year while debt is a snapshot at the end of year, so it's preferable to use an average of the start- and end-of-period debt instead.

In the case of Equifax, their Revenue-to-Debt ratio for FY2018 was 1.56 (Equifax, 2018). This means that, if all debt was to increase in cost by 40bps the effect would be that 25.6bps of revenue would be required to service this cash flow drag. Such impacts can quickly degenerate profitability and weigh on investor sentiment, before even considering the much starker ratings differences such as the 500bps for transitioning from "BBB" to "CCC".

Indebtedness can also have a significant impact. When looking at the FTSE350 as a sample, approximately 20% of constituents hold no long-term debt (Stockopedia, 2019), effectively insulating them from Credit Rating implications (assuming no change to capital structure). Simultaneously, these are predominantly Financial Services companies such as fund managers, arguably making them prime targets for cybercrime.

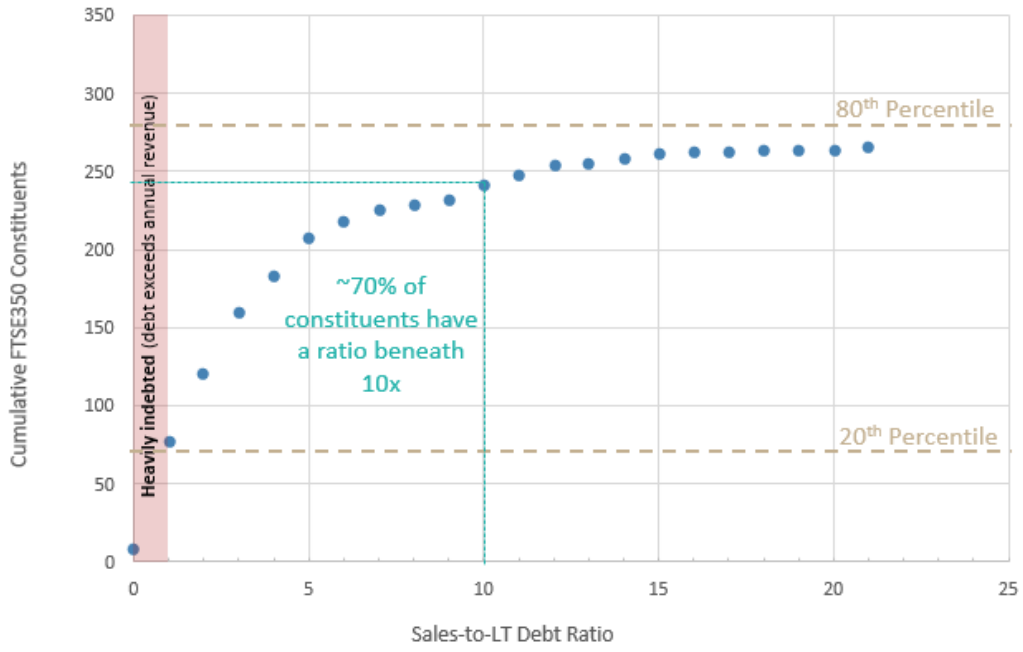


Figure 3-10 - FTSE350 Constituents' Sales-to-LT Debt Ratios. Data from relates to 2018 Financial Year

At the other end of the spectrum, a different 20% of constituents are so heavily indebted that for every pound[6] of revenue, they hold at least one pound of debt. Overall, 70% of the companies in the FTSE350 have at least 10 pence of debt for each pound of revenue. Such figures may prove useful when equating revenue impacts to debt and credit ratings. It should be noted, however, that such ratios are idiosyncratic, without distinguishing profitability, cash flow robustness or most notably capital structure choices, as laid out by (Modigliani & Miller, 1958).

[6] Currencies have been converted where applicable for analysis in this report, but financial ratios are typically unaffected by such conversions.

4 Cyber Risk and Cyber Insurance Modelling

4.1 Modelling Literature Review

A robust framework is desirable when building and analysing models and one such example is provided by (Böhme & Schwartz, 2010), who use it to compare a variety of models in literature. The framework is composed of 5 elements, shown below, though it should be noted that not all elements are present in all models.

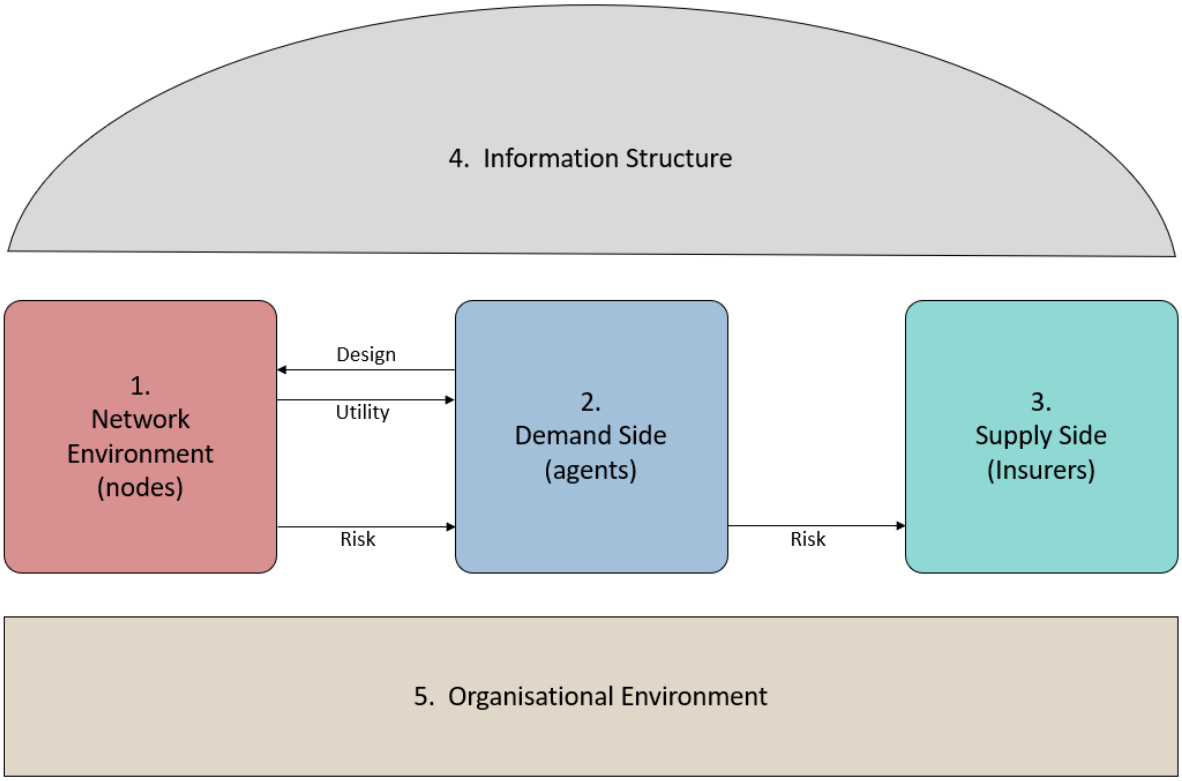


Figure 4-1 - Modelling Framework proposed by (Böhme & Schwartz, 2010)

Elements may exhibit a range of complexity as well as utilise different model paradigms. It is also possible for a single model to exhibit significant overlap or interrelationship between elements, particularly those of the information structure and organisational environment

The great variety in design of models make categorisation difficult, though one taxonomy (Wolthusen, Unit 5 - Critical Infrastructures and Dependencies, 2019) calls for three high-level categories; Graph-based, Game Theory and Agent-based models. Again, there is overlap and the opportunity for hybridisation, with no purely Graph-based models[7] encountered. Instead, Game Theory or Agent-based approaches which incorporated graphs as part of their operation are used.

Among Game Theory models there are two prevalent approaches, one based on a "single shot" while another looks at repeat-game equilibrium. The former is infrequently used in literature, in preference for the latter which provides probabilistic findings that are more generally applicable, though less definite.

[7] For clarity, Graph-based models are those which rely solely on the weight of edges to determine model behaviour. While other approaches may utilise a graph, model behaviour is determined by defined functions.

An example of one of the simplest Game Theory model types, a single-shot Game Theory model with two players, is used in a paper by (Laszka, Panaousis, & Grossklags, 2018) in which they look at the risk of Insureds succumbing to Moral Hazard. They find that in theory the insured will always misreport, while the insurer should never find it worthwhile to call an audit to identify this misreporting.

Another Game Theory paper by (Cartwright, Hernandez-Castro, & Stepanova, 2018) analyses rational outcomes of ransomware. They find that in theory the attacker should always accept a non-zero ransom. Furthermore, when paid, they should never destroy data out of spite.

Such outcomes would come as little solace to the significant proportion of malware victims who lose data after paying when impacted by ransomware such as "Ranscam", designed explicitly to delete files after ransom payment (Brumaghin & Mercer, 2016). It also serves to highlight one of the constraints of Game Theory – results can be unusual because they are purely rational under the assumptions of the model. Unfortunately, as the field of Behavioural Economics has found over the last 5 decades (Kahneman & Tyversky, 2011), the rational person is often quite rare in relation to those influenced by heuristics and biases.

Hybrids of Game Theory and Graph models exist and one proposal has been made by (Insua, Couce-Vieira, & Musaraj, 2018), though results and output are the subject of subsequent papers. The principle is that a directed graph governs the nodes that the players can attack or defend, information and approaches available for use. Capture of nodes would result in Utility, which the players seek to maximise.

A natural use for this type of model is an attacker/defender game, with cyber insurance applications. The reinsurance game uses a single player to move through a graph of utility vertices that may add or destroy value, depending on whether they are portfolio synergies or threats. The insurance coverage game is once again adversarial, with the insurer and insured competing to maximise utility through commercial nodes.

While this model is an intriguing concept, it is unproven and likely to involve significant setup of a landscape that is both dynamic and difficult to quantify. The follow-up papers with results will certainly be worth checking in due course.

Agent-based models utilising graphs have seen widespread use, with (Laszka, Johnson, Grosklags, & Feleghyazi, 2014) identifying three common approaches.

The first quantify impact as simply the proportion of healthy vertices to unafflicted ones, with recovery mechanisms optional. A model of this type is used in their paper and compromises vertices randomly before propagating only to immediate neighbours, a limitation in place to limit epidemic spread. Quantification was based on percentage of nodes compromised in a sample subset due to the NP-hard nature of the problem and the fact that some network datasets are extremely large[8].

The second approach replaces the binary outcome with a value distribution for each node, though propagation of infection is still deterministic. While examples are cited in their paper, they are relatively uncommon now as they've been superseded by the third type.

[8] The AS dataset used was ~41,000, while the Facebook dataset was ~1.2 million users

The third class is of epidemic models, in which nodes move through the Susceptible-Infected-Susceptible cycle using arbitrarily complex mechanisms to determine infection. (Xu & Hua, 2017) utilise such a model in their paper for the Society of Actuaries, which ran a Monte-Carlo simulation of 365 steps per iteration and these iterations would build a distribution. Node compromise occurred with random probability and, once compromised, vertices could be cured after a one period delay. However, the added complexity of the model highlights the trade-off that must then be made to graph size, which in this case is perhaps too low at only 10 vertices. Each compromise resulted in a variable value impact and the sum of all compromises in the year resulted in the insurance value.

Other models in the field use variations on the themes above, with adjustments to suit the focus of the analysis in question. For example, (Fahrenwaldt, Weber, & Weske, 2018) focus on network topology and use graphs of a fixed number of vertices while tailoring edges. The compromise process bears similarities to that used by (Xu & Hua, 2017) with infection propagation occurring between neighbours on each step, but inoculation occurring with random probability and no propagation mechanism. Compromised vertices may therefore take an arbitrarily long time to fix.

While a fixed duration may be commensurate with a detection-patch cycle, it doesn't account for the compromised period prior to detection. A random duration better handles the potential for undetected compromises. Neither approach really address the plausible behaviour of a sysadmin to patch all systems under their control (i.e. a subgraph) upon detection.

Finally, one model used by (Shah, Dahake, & Haran, 2015) is worth mentioning because it is both simple and in effect operates in reverse. It uses known values for insurance premiums in order to back out the implied value placed by customers on their security and privacy. Such approaches are important decision-making tools in commercial instances where the "value" is known but critical variables are not and may also be used as a sense-check.

5 Model Overview

In order to analyse the possible properties of a Cat bond a model has been developed, called SafetyNet in acknowledgement of the security Insurers seek when writing policies and the connected nature of the Insureds they cover. This model (henceforth referred to as SafetyNet) can be summarised in the framework used by (Böhme & Schwartz, 2010) as shown below and may be made available on enquiry. Following a review of the literature, it is designed in a similar fashion to that used by (Xu & Hua, 2017), which will be referred to as the reference model.

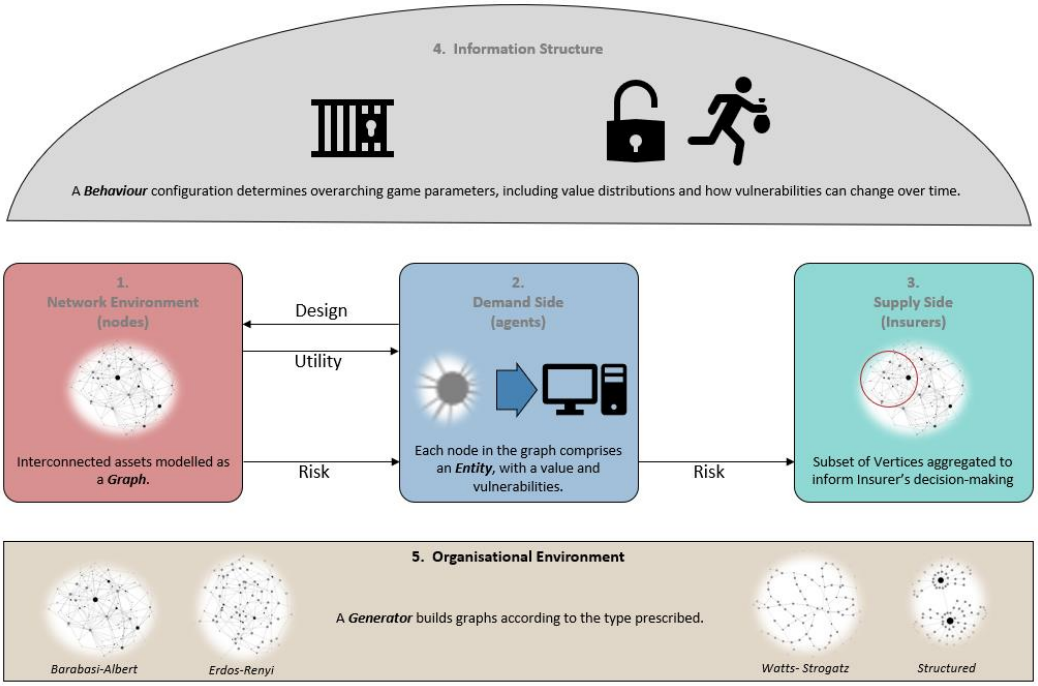


Figure 5-1 - Summary of the SafetyNet model using the framework from Bohme & Schwartz' paper.

The reference model was selected due to the relative flexibility of approach and potential to resemble reality. As a Monte-Carlo approach there are further practical benefits, insofar as probabilistic models are now generally understood in business. Furthermore, the publishing of this approach by an institution related to industry also provides a level of endorsement.

SafetyNet operates on an annual timeframe, conducting 365 steps within a contiguous state before resetting key variables and starting a new iteration. This timeframe aids understanding, with direct comparability to per annum statistics, and is a common timeframe for business decisions. While the number of iterations may be adjusted, analysis will be performed with a sample size of 10,000. The incentive to choose this is less due to a desire for precision and more due to the increased opportunity for outlier results that comes with more iterations. After all, where catastrophe is concerned, outliers are precisely the area of interest.

At the heart of SafetyNet is a graph, in which the nodes are connected by edges representing the network connections of systems or businesses. Associated with each node is an Entity, configured to represent the impact costs and likelihoods for the underlying object it represents, whether it be a single system or an organisation. While the details of SafetyNet are in some cases tailored to a single business and effects on an organisation-specific Cat bond, many of these aspects can readily be adjusted to look at wider issues. Opportunities for future expansion will be covered in the discussion.

5.1 Threat and Vulnerability Framework

With regards to the Threats posed, the Threat Landscape by (ENISA, 2019) was used as a basis, but these threats were categorised as shown in Figure 5-2. As the ENISA Threat Landscape has a different target audience than is needed in this instance, some summarisation has been performed. The focus on malicious threats means that simple accidental threats are omitted, while the inclusion of threats to the individual may not be of direct concern to an organisation, or covered elsewhere in the model.

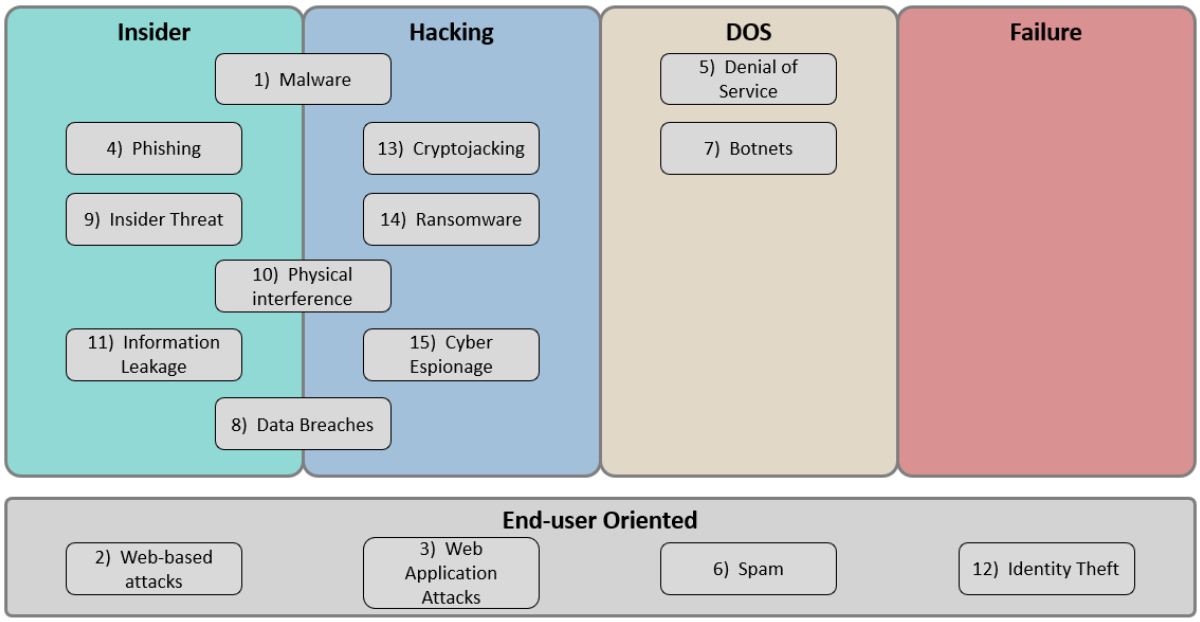


Figure 5-2 - Mapping of ENISA Threats to Model Mechanisms

As can be seen above, Failure has been explicitly included in the model as it's pervasive, impacting businesses irrespective of their network configuration. According to some sources, "system glitch" should be a serious concern to Insurers, with a (NetDiligence, 2018, p. 27) study finding it to be the single largest cost on average by a significant margin[9]. However, a look at the underlying data suggests this is a case of the "flaw of averages", with a single very costly incident causing the average across a very small number of cases to be unusually high.

Several threats, categorised as "End-user Oriented", are indirect and are thus incorporated in other categories. Repercussions from Identity Theft, for example, would predominantly fall under Insider Threats. Successful attempts at Web-based, Web Application attacks and Spam (itself connected with Phishing) would lead to Hacking.

As with the Reference model, two impact mechanisms are in play – a random selection mechanism followed by a propagation mechanism. The random selection is the first to run, using high level probability of occurrence to determine whether an incident will happen on a given day. If this occurs, victim nodes are selected, and impacts applied.

[9] Average cost of a system glitch was $19.5M USD, with Malware in second place at only $1.2M USD.

These random selections are considered independent for the purpose of modelling, though this may not necessarily be true. As can be seen from Figure 5-2, there is some crossover. Malware, Insider Threat and Phishing may all be interrelated, with Phishing leading an Insider to initiate a Malware attack. The model, however, would not consider this sequence of events. Instead this sequence would all simply be categorised under the broad category of a Hacking incident and valued accordingly.

For the purpose of SafetyNet, the scope of Insider Threat has been limited to isolated malicious and unwitting compromise of information or direct loss of funds. The former may include pre-meditated information theft and industrial espionage, while the latter would include accidental compromise of information or being a victim of a CEO Fraud e-mail and transferring funds.

This overlap may in turn can lead to over- and under-estimation of costs in the model. Overestimation may arise where one category would preclude another. While unlikely, a DDoS attack that happened to coincide with an Insider falling victim to a phishing attempt, for example, may be beneficial. Conversely, underestimation may arise if an organisation became the target of sustained compromise attempts, with Insider vectors and hacking attempts occurring in parallel.

The propagation mechanism differs significantly from that described in the Reference model as well as any other model encountered in literature. Instead of probability-based propagation or deterministic propagation simply limited to one hop each round, this model uses an adversarial approach, allowing for highly interdependent epidemic spread if left uncontrolled, while having very limited impact if controls are in place. This approach was chosen in order to better accommodate the potential for overwhelming spread of malware that has been seen in attacks such as WannaCry, NotPetya and GandCrab.

An overarching Master Vulnerability Set, held within the Behaviour of SafetyNet, contains the reference set of all Vulnerabilities that can exist. From this, each Entity receives a subset of vulnerabilities which it holds within its Defender and is only vulnerable to this set. Attackers on the other hand are generated when a Hack event occurs and are created with a separate random set of exploits for these vulnerabilities.

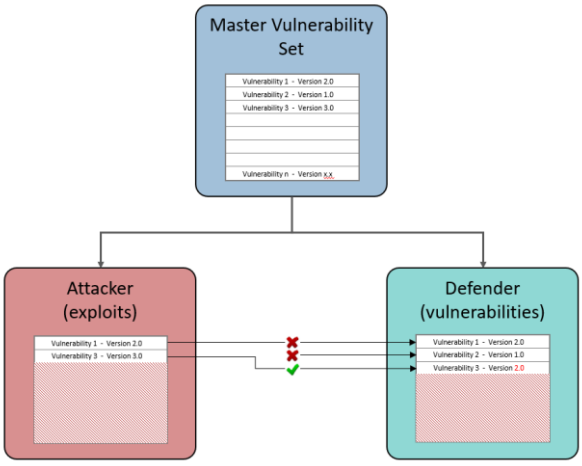


Figure 5-3 - Example Attacker/Defender Comparison Contest

When an Attacker tests a Defender, as represented in Figure 5-3, it succeeds only if the Vulnerability matches that of the Defender, and the Attacker's version exceeds that present in the Defender for

the corresponding Vulnerability. Consequently, in the example above, the Attacker would succeed in compromising the Defender because the defender has Vulnerability 3 at version 2.0, while the Attacker can exploit up to Version 3.0. An attack on Vulnerability 1 was defeated and the Attacker did not hold an exploit for Version 2.0.

Within these agents, Vulnerabilities are held in a hash table, allowing Attackers and Defenders to be tested rapidly without repeated iterations over lists. If a Vulnerability is tested and a value is returned, the Vulnerability must exist. If nothing is returned, the Defender is not vulnerable.

An update schedule has been incorporated into the model, with update probabilities based upon statistics from (Akamai Technologies; TechValidate; Applause, Inc., 2019). This approach allows for an arbitrary window of vulnerability, but for the purposes of the analysis later, this window is fixed to one game-day.

The pseudocode in Figure 5-4 summarises the above description, showing the sequence of events in the model.

```
1:    WHILE i < iterations do
2:      WHILE t < 365 do
3:        Increase Master Version register
4:        FOR each node
5:          Apply Updates based on Entity patching behaviour and check Attacker register
6:        FOR each incident category
7:          IF category deemed to apply, select victim nodes
8:            Apply impact costs to victim nodes (except Hacked)
9:            IF Hacked and the victim node is susceptible, add node to the Propagation Stack
10:       WHILE Propagation Stack is not empty
11:         Pop node from the stack
12:         Apply impact cost
13:         FOR each node in Neighbour Set
14:           IF node is susceptible, add to Propagation Stack
15:       FOR each node
16:         Evaluate total node impact
17:         Export total to OUTPUT
18:       Reset values for next t
19:     Reset variables for next i

OUTPUT:  Total loss per node for the year, for each iteration.
```

Figure 5-4 - Pseudocode for the sequence of events in a complete run of SafetyNet

5.2 Parameters of the Model

This section concerns the model parameters that are intended to comprise the baseline configuration and remain consistent throughout SafetyNet.

Despite the presence of limited directly applicable data, quantification of information security risks is a significant improvement over qualitative approaches. As (Hubbard & Seiersen, 2016) make the case in their book, there are a couple of notable benefits to decision-making that arise.

First, quantifying values offers a degree of reproducibility which, as more information becomes available, can be built upon to improve accuracy. Second, an inaccurate estimate that is known to be either too high or low can provide a useful yardstick against which to measure decisions. The "Rule of 5" is worth highlighting – "there is a 93.75% chance that the median of a population is between the smallest and largest values in any random sample of five from a population".

In the context of a model describing the value loss of a single business, a universal parameter that typically scales with the business was needed, logically leading to revenue. While there are anomalies such as start-ups, most organisations are premised on revenue, irrespective of whether they are businesses or charities.

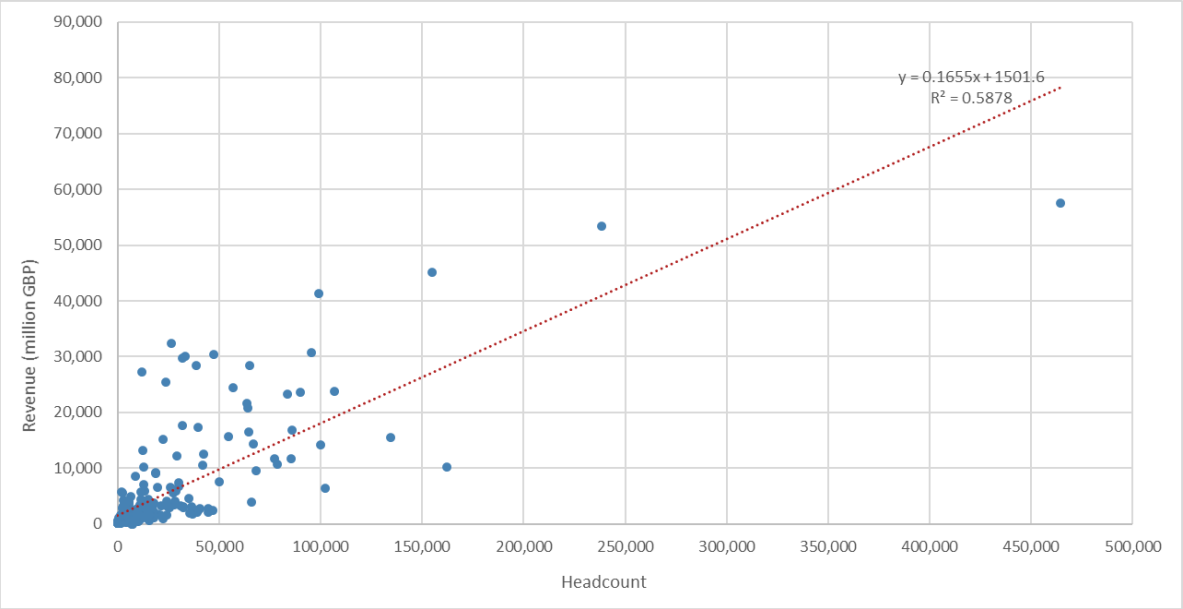


Figure 5-5 - Revenue vs. Employee Headcount for the FTSE350

The chart in Figure 5-5 shows the relationship between revenue and headcount for 347 of the companies in the FTSE350[10]. While far from perfect, it does show a moderate correlation between headcount and revenue with ~59% of the variance in the revenue figures explained by headcount. Therefore, this relationship will be used as a bridge between per-user figures and dollar values, proving invaluable going forward.

With that in mind, it's assumed that all vertices contribute to revenue, resulting in a sum-of-parts total. As not all systems are equal, the question is how this value is to be distributed. It has been assumed that vertex value is on an exponential distribution, with most vertices contributing below-

[10] Employee data from (Citywire, 2019)
Revenue data from (Stockopedia, 2019)
BP, Shell and Glencore have been omitted from the trend as their magnitude and capital-intensity is disruptive to regression.

average value while relatively few vertices make large contributions. The mean of this distribution has been set to 1.0 for convenience but is largely irrelevant – percentages can be determined by relating the node value to the total.

5.2.1 Hacking Incident Impact Parameters

The first category has been treated differently to the others as, unlike all further categories, the probability of hacking will be considered a variable for further analysis. This is because the available data shows that an Insured's industry can have a significant impact on the frequency of hacking experienced. Additionally, as the model differentiator is the propagation system linked to hacking, this also warrants checking the sensitivity to the underlying probability.

One parameter regarding the susceptibility of a Defender will remain fixed in all runs and that corresponds with the chance to patch vulnerabilities. This has been set to occur notionally at the end of the step, while Attackers will use the latest updates from the start of the step. As impact statistics relate to per-hack values, this configuration means that each attack has only one opportunity for the attack to succeed before it is patched. This approach can be refined if reliable data regarding patch frequency and cost accrual from dwell-time existed.

Impact of hacking, on the other hand, is consistently modelled throughout all cases and based on information in a report by the Ponemon Institute for (Accenture Security, 2019). As with other datasets, this one shows relative costs of certain attack types, but what sets it apart is that the descriptive text provides enough information to propose a sense of scale for analysis.

The relative data shows that the topics of interest for SafetyNet's categorisation contribute an impact of $3.3M to the total impact costs of $13M on average, comprised of $2.7M due to Malware and $0.7M from Ransomware. Thus, ~25% of the costs considered in this report are attributable to activity falling under "hacking" category in SafetyNet.

In isolation, this provides little information on what basis the "average" has been calculated, but this report makes reference to the average revenue at risk for "…an average G2000 company – with 2018 revenues of US$20 billion…". This annual average of 2.8%, in combination with the relative percentage above, implies an average of 0.71% of revenue is at risk.

This average is assumed to be the mean of an Exponential distribution ~EXP(0.0071), with a high frequency of lower impact incidents. There is also potential for infrequent incidents of much higher value, allowing for calamitous events such as those that befell AMCA or Experian, as well as allowing for the potential costs of breaches under GDPR with its cap of 4% of revenue. In fact the maximum may be even higher, with the recent fine imposed on Facebook by the FTC equating to 9% of global revenues.

5.2.2 Failure Incident Parameters

It has been assumed that the epicentres of value, per the above, are servers as opposed to end-user computers. This stands to reason for both technology-based companies, whose revenue streams would be generated from server availability. Other sectors are likely to follow this distribution too, with critical information (ideally) held in relatively few nodes rather than liberally distributed across the network.

Therefore, uptime is less likely to be driven by failure rates of consumer equipment than by statistics for server hardware. To this end, one such source is provided by (Panasonic, 2019), who published data on the failure rates of servers by age. Each individual vertex is then tested against these failure rates daily and it's assumed that systems are evenly distributed across this age distribution, from 0 to 7 years old.

When a failure occurs, the impact is based on a distribution sourced from (Unitrends, 2018). The data follows a discrete distribution of Recovery Time Objectives (RTOs), varying from 4 hours to 2 days. When applied to a node, this will result in a value impact to that specific vertex of the proportion of the year that the downtime caused.

It's acknowledged that the sources of data above may have vested interests in the provision of such information but given the low frequency and impact of these figures, it's unlikely this category will cause value loss on the scale of other categories. It is nevertheless possible for large companies with concentrated value nodes to reach the large absolute costs mentioned in the NetDiligence report to occur.

5.2.3 Denial of Service Parameters

Most information regarding DoS attack frequency are provided in aggregate with no distinction regarding target, efficacy or geographic scope. Without insight into a suitable denominator, as was fortunately the case for Hacking incident probability, it is not possible to convert them into a frequency for use with the model. In the case, quantification may be indirectly possible via data from (Action Fraud (UK), 2018), who provided absolute numbers of actual DoS attacks (as opposed to extortion attempts) in relation to hacking attempts on servers.

As previously mentioned, hacking frequency is a variable of interest so it's important that the two are deconvolved in order to prevent value impact of changes to hacking frequency being affected by collateral impacts to DoS impact likelihood. This has therefore been modelled as a convolution of two distributions that will remain unchanged to ensure independence going forward.

Data from the Commercial Victimisation Survey (CVS) by (UK Home Office, 2019) shows that, on average, 3.42 hacking incidents occur per business in the UK and Wales. Each step has an underlying chance of 0.00937%, equating to a Binomial distribution of ~B(365, 0.00937).

The Action Fraud dataset shows that the number of DoS attacks have ranged from 45% to 97% relative to those of hacking. This is therefore the basis for a Normal distribution of ~N(0.71, 0.13) in which these extremes are captured within 2σ of the mean.

The combination of these two distributions allows for the incorporation of this relative data while also maintaining independence from the hacking probability variables themselves in the model.

Impact from DoS attacks has been related to downtime, for which binned data is available in a report by (Kupreev, Badovskaya, & Gutnikov, 2019) at Kaspersky. It follows a Lognormal distribution ~ LN(0.1, 1.7) for which a cumulative distribution fitting curve is provided in Figure 10-2.

Due to the uncertainty regarding the scope of a DOS attack, delineation has not been made regarding the quantity of affected nodes. While DoS attacks are unlikely to impact the entire network, there is no reliable information on which to base any limitation to scope, and even targeted DoS attacks would likely impact the highest value nodes, such as customer-facing servers.

5.2.4 Insider Threat Parameters

When it comes to Insider Threats, (Ponemon Institute, 2018) produces an annual report of threat statistics. Some graphs in the report are of less use than they could be as they use a discrete case axis and therefore lose the potential to determine regressions or a sense of relative organisation scale (examples are shown in Figure 10-3). One graph was of particular use though and has been reproduced below, incorporating extrapolations using the Revenue vs. Headcount relationship shown previously. The original chart is shown in Figure 10-4.

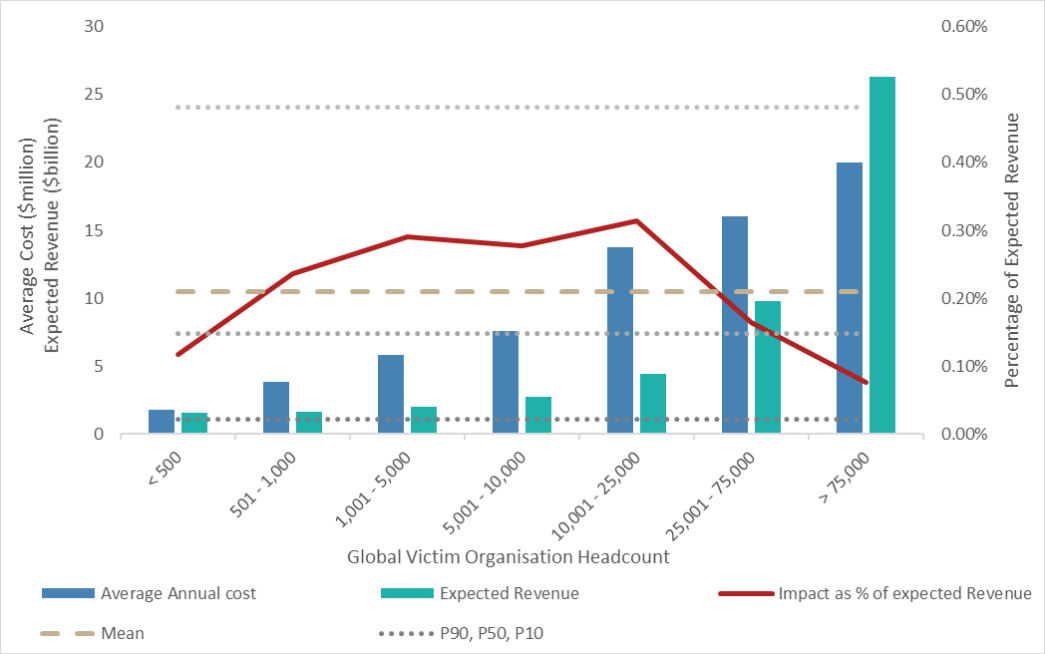


Figure 5-6 - Insider Impact as a Percentage of Expected Revenue. Based on data from (Ponemon Institute, 2018) combined with Figure 5-5.

Insider Threats are not limited to the node on which the act is committed. In the case of malicious insiders, data may be harvested from servers while unsuspecting insiders may simply transfer funds to fraudulent bank accounts, again exceeding the individual value ascribed to a node. Therefore, the impact is measured as a percentage of total revenue (i.e. the sum of all vertices in the graph).

Across all headcount categories, the average impact in terms of Expected Revenue (backing out a revenue figure using the headcount relationship) is 0.21%. This has been used as the mean of an Exponential Distribution ~ EXP(0.0021) with the corresponding percentiles of P90, P50 and P10 represented in Figure 5-6 too.

While the Ponemon report is a useful dataset for impact, it is not suitable for incident frequency. The report is based upon a survey of victims and therefore is already a pre-selected sample with no means to derive a baseline incident rate across all businesses. Instead, frequency data is based on a separate source by (CA Technologies, 2019).

The data itself can be fitted with a Lognormal distribution ~ LN(0.35, 2.05) with a -1 shift and floored to 0, allowing for businesses that have zero incidents. The resulting number of annual incidents is then calculated as a per-diem rate and applied each step.

5.3 Variables for Analysis

With the above parameters fixed across all runs, each of the following changes will be made individually in order to isolate their effect on results.

As the model is probabilistic, there will be some limited discrepancy between runs simply due to different random number generation, but the overall effect of this should be small in relation to the changes to the model variables.

5.3.1 Effect of Hacking Incident Probability and Underlying Propagation Probabilities

The dataset published by the (UK Home Office, 2019) provided the aggregate hacking data on which DoS probabilities were based, but it also highlighted an interesting disparity. The data covered four different sectors[11] with a very distinct bimodal distribution. This is likely to be an artefact of their reliance on technology, susceptibility to attack and value as a target.

However, the fact that there is a clear distinction, with Wholesale, Retail and Manufacturing suffering nearly 5 times the number of hacking incidents as the other sectors, warrants further investigation. Such a distinct difference could have very significant implications on insurance premiums for the respective sectors.

The probability of hacking in SafetyNet shall therefore be fixed at an effective annual probability of 5.5 hacks per year for one run and 1.2 hacks per year for the other in order to identify any effects this may cause. These correspond to the two extremely prominent modal values corresponding with the two pairs of sectors.

The absence of any reliable information regarding the success rate of hacking incidents to events makes the determination of probability difficult. In the case of SafetyNet, this probability is a function of the number of vulnerabilities on the Defender when compared to the number of exploits of the Attacker and results in the collision probabilities in Figure 5-7.

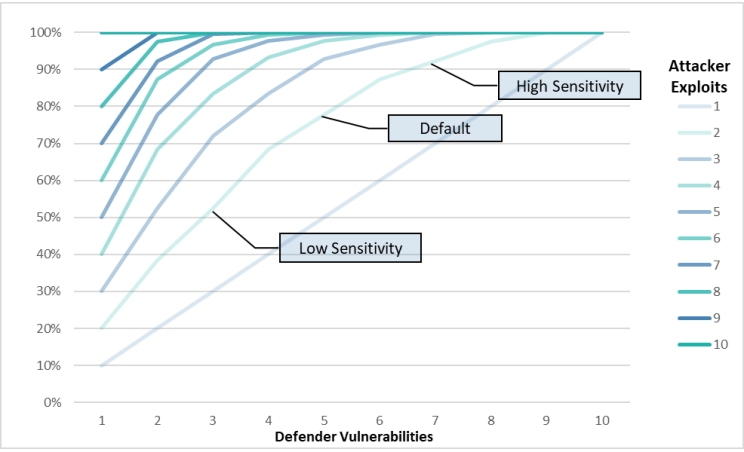


Figure 5-7 - Attacker Exploit vs. Defender Vulnerability Collision Probability

The default selection of 5 vulnerabilities and 2 exploits results in a 78% chance of collision, while sensitivities at 3 and 7 vulnerabilities have a 53% and 92% collision probability respectively based on

[11] The categories are: Wholesale & Retail; Manufacturing; Agriculture, Forestry & Fishing; Arts, Entertainment & recreation.

the formula below. The associated decision tree shows how this formula arises, as it is the combination of the two green branches. It may also be extended to cover further threats as needed.

$$P(x) = \frac{v}{n} + \left(1 - \frac{v}{n}\right)\left(\frac{v}{n-1}\right)$$

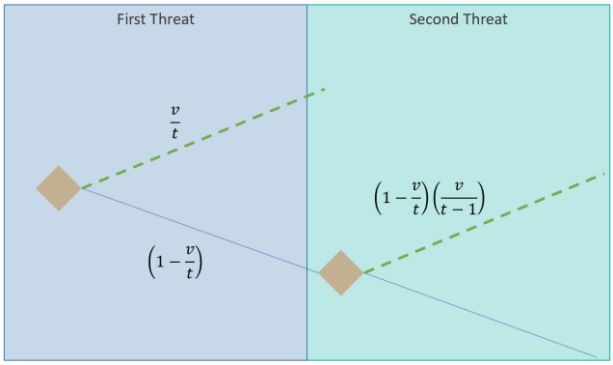


Figure 5-8 - Formula and Probability Tree for Two Threat Cases

5.3.2 Effect of Monoculture

Another sensitivity is related to the numerous cited sources concerning the abnormal risk that monoculture places on Insurers, so a sensitivity will be run regarding a monoculture risk. While much of the concern for Insurers is for monoculture at the portfolio level, the scope of the model will look at this same risk within a modelled organisation.

To achieve this, no change to the underlying probabilities will be performed, but instead one of the otherwise random risks for all vertices will be held constant, resulting in a single point of failure which may be exploited and propagated across. Such an occurrence may represent a common operating system or hardware vulnerability for which a zero-day is discovered.

Other models in literature commonly utilised two probabilities, *p* and *q*, to determine random infection chance (based on *p*) followed by infection propagation chance (based on *q*). To put this in context, such a change maintains p in the region of 3.8%, assuming 5 vulnerabilities per Defender and 2 threats per Attacker. However, upon infection there is a 1-in-5 chance that the infection will propagate unhindered throughout the network. A sensitivity will be run to determine the impact of this type of behaviour arising from monoculture.

5.3.3 Effect of "Hardening"

One common method of improving network security is hardening, in which the purposes of a given node (e.g. server) are either limited or unused ports are closed. This can shut down potential vulnerabilities and attack vectors, and the mechanism can be readily modelled within the framework of SafetyNet. This can be performed by reducing the vulnerabilities within the Defender of selected nodes to a reduced set, which for the sake of these runs will be reduced to a single vulnerability.

Instead of random selection, which is unlikely to be how hardening is carried out, SafetyNet will apply hardened nodes in order of their respective *degree*, or number of connected edges. For the

purpose of this sensitivity, 5% of nodes will be hardened, effectively reducing the ability of infections to propagate through the graph (and of course initially infect) the graph.

5.3.4 Effect of Graph Structure

The first sensitivity to consider is the structure of the graph itself. Social network and Internet topographies have in the past been modelled as randomly generated graphs using algorithms such as those by Erdős-Rényi and Watts-Strogatz. More recent developments include the scale-free types of graph such as those using the Barabási-Albert (BA) approach, which it's been postulated is a better approximation to the structure of the internet.

All these approaches are implemented in SafetyNet, but as the Barabasi-Albert graph is well-regarded as an appropriate proxy for network graphs, it will be used as the underpinning for most of the sensitivity runs. In order to minimise moving parts, one BA graph will be generated, and its properties will be adjusted to suit the sensitivity.

Despite this selection, it should be noted that the artificial construction and commercial agreements underpinning the internet mean that in reality it's more structured than a randomly generated scale-free graph would be (Wolthusen, 2019, p. 18). Furthermore, as the scope of this analysis is an organisation, network structure is likely to be architected and thus very structured. As a result, one further custom algorithm has been included for analysis, the pseudocode for which is in Figure 5-9.

```
1:    FOR number of hub nodes
2:      Create a node
3:      FOR each other hub node, create an edge
4:    WHILE total nodes < desired total nodes
5:      Choose a hub node
6:      WHILE a settling point has not been chosen
7:        IF node is chosen for settling
8:          Create new node and create an edge to settling node
9:        ELSE
10:         Choose new node that hasn't already been visited
11:         Increase probability of settling

OUTPUT:  Complete graph
```

Figure 5-9 - Pseudocode for the creation of an extremely structured, tree-like graph

This algorithm creates a nucleus of *m* meshed nodes, ostensibly the gateways of regional offices interconnected via the internet itself. For each further node to the total *n* nodes desired, it chooses one of these hub nodes as a starting point and selects a non-hub branch to follow. It will follow this branch, with *j/k* chance of settling as a neighbour of the current node, where *j* is the number of jumps it has performed thus far and *k* is the maximum depth of the graph. Thus, when it reaches the maximum depth, the chance of settling is *k/k* = 1.

A run will be performed on a graph created using this algorithm in order to identify the effects of this structural change.

5.3.5 Effect of Graph Scale

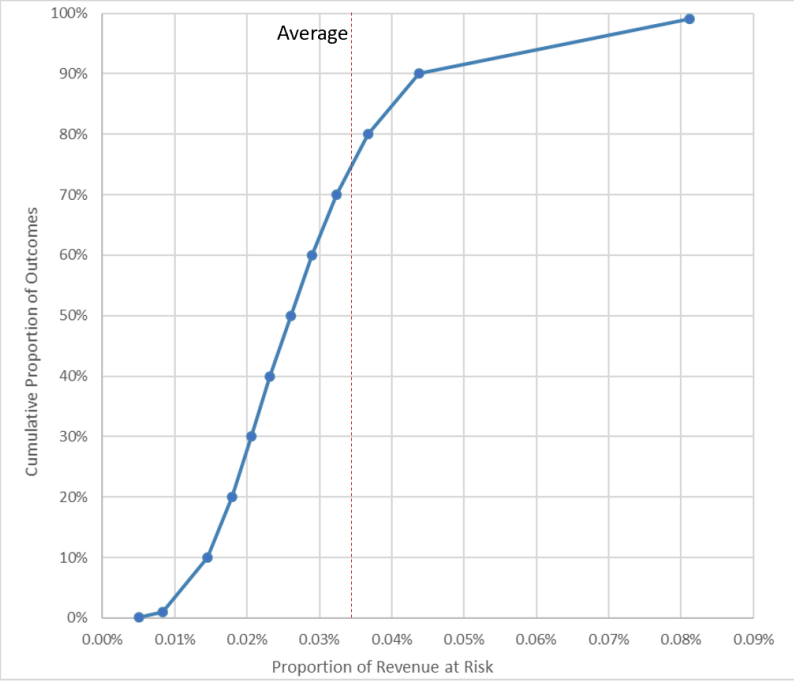
An important sensitivity for practical purposes is the effect scale may have on output. To investigate this influence of scale, sensitivities shall be run at a scale of 100 and 10,000 nodes, an order of magnitude higher and lower than the base case of 1,000 nodes.

It's important to note that scalability will likely be reliant on the underlying graph structure which, as mentioned previously, is using the Barabási-Albert generation algorithm, is theoretically scale-free. Therefore, this sensitivity is to determine whether there is any reason for the output to distort despite the scale-free properties of this graph structure.

6 Results

This section contains the output of the modelled cases as described above, as well as some supplementary runs where available in order to better inform findings. While some cases require further explaination, the wider application of these results will be handled in the Discussion. A table of results from the primary runs is available in Appendix 10.4.

The output of the model comes in the form of a revenue impact for each iteration, along with the total network revenue figure, allowing for numbers to be stated in terms of percentage of revenue lost. This normalisation will help make numbers comparable across runs and even graph sizes. The metrics of mean (μ) and standard deviation (σ) are necessary for the application of the aforementioned Standard Deviation Premium Principle for premium calculation.



	Base
Average	0.034%
Std. Dev	0.127%
Min	0.004%
P99.9	0.005%
P99	0.008%
P90	0.015%
P80	0.018%
P70	0.021%
P60	0.023%
P50	0.026%
P40	0.029%
P30	0.032%
P20	0.037%
P10	0.044%
P01	0.081%
P0.5	0.315%
P0.1	1.518%
Max	6.369%

Figure 6-1 - Results from the Base Case

Data from the Base case shows that the Expected Losses from SafetyNet are just over 3bps. Superficially, an Expected Loss approach in this context may seem appropriate as it would seemingly result in the Insurer making a loss only ~25% of the time. However, this difference between the P50 and the percentile approximating the mean is just one of several red flags that indicate an unusually skewed distribution.

The σ of 12.7bps also highlights this concerning property. As this data has a definite floor of zero, even a third of one σ below the mean is impossible, implying the variance in the data causing this resides above the mean. This elevated σ also suggests that conventional values of safety loading appropriate for more normally distributed risks will lead to extremely expensive premiums. Conversely, using the above case and a target risk of ruin of 95% the appropriate safety loading would be only λ=0.2. Contrast this with a Normal distribution, in which a 95% risk of ruin would give rise to a safety loading of 2.0.

In the above chart the final percentile has been omitted to make the scale meaningful, but compromising at the P99.5, the level set for the SCR threshold, is a good compromise as it avoids the extreme volatility of the maximum value. With this adjustment, shown below, the skewness becomes apparent.

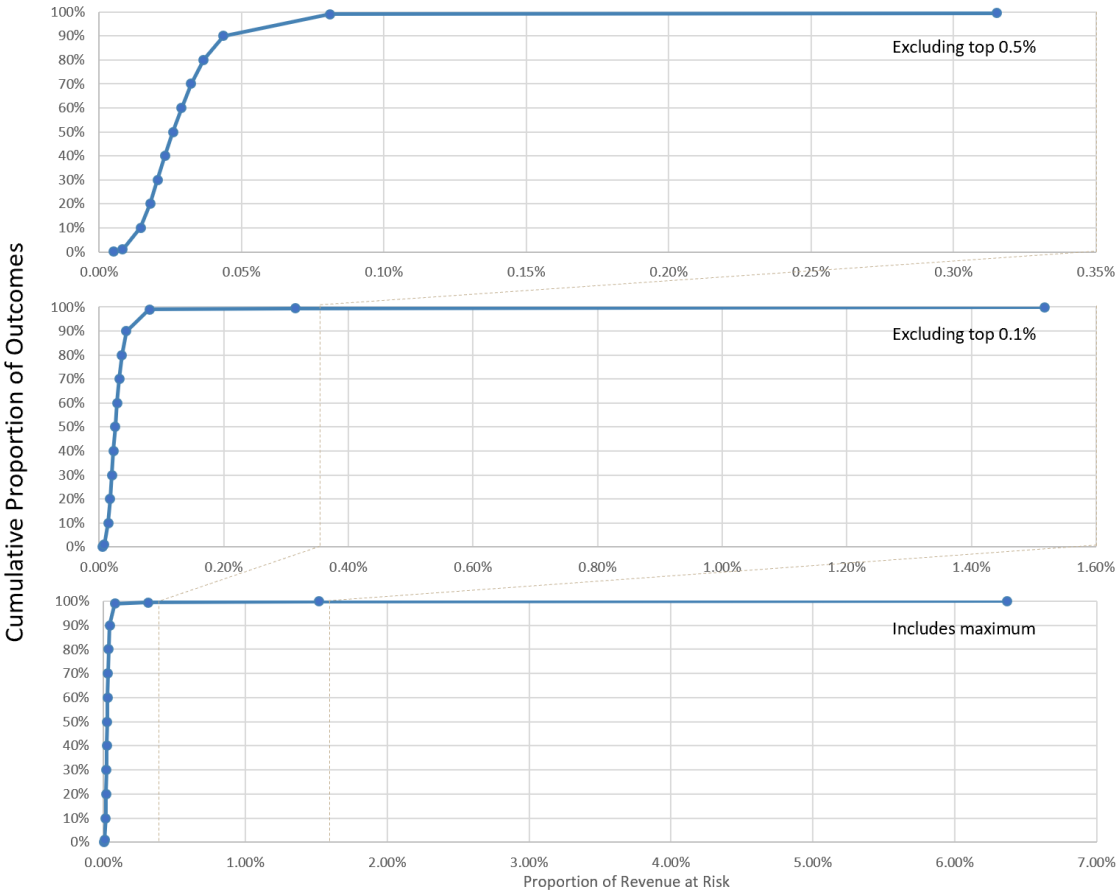


Figure 6-2 - Results from Base Case, including upper percentile figures

Assuming the Insurer seeks coverage to the SCR threshold from safety loading alone, this would lead to a multiple of around 2.3, which may go some way to explaining the higher premiums reported by Tondel et al.

6.1 Impact of Infection Probabilities and Propagation

Several sensitivities were run regarding the impact of hacking probability and propagation through the graph. The results for these runs are shown in Figure 6-3, but the outcome appears somewhat surprising at first glance.

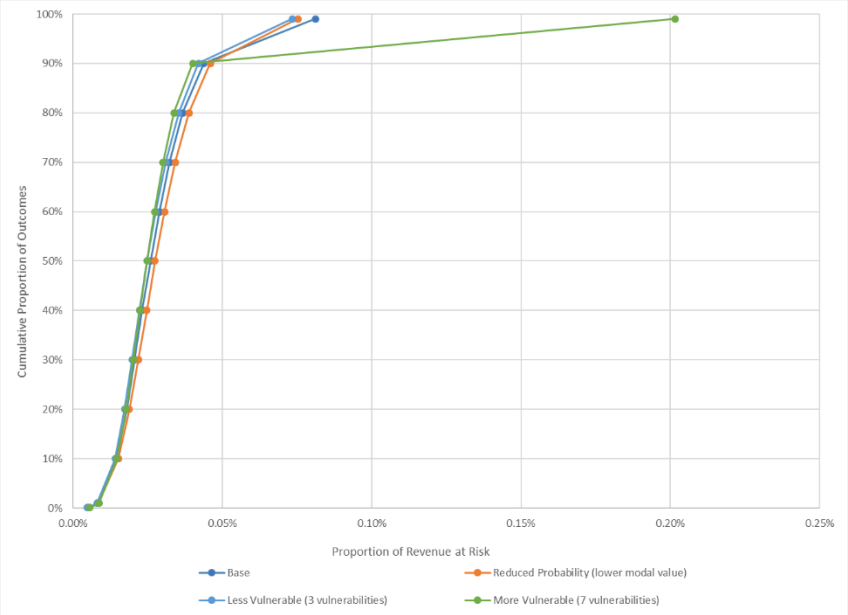


Figure 6-3 - Results from Sensitivity to Infection Probability Changes

For much of the cumulative probability, the outcomes are ordered in such a way that they bear little relation to the underlying sensitivity. Reduced infection probability cases incur higher losses than the Base, while the case with increased vulnerabilities is the least impacted for most of the distribution. It is only in the final percentiles that the order one would expect begins to occur, with reduced infection rate and vulnerability cases being least impacted and the increased vulnerability case showing more notable losses.

Given the irregularity of these results, a selection of runs were performed to confirm the model was working as intended. Therefore, the runs were repeated with only the Hacking category enabled, enabling the relative impacts of these runs to be isolated.

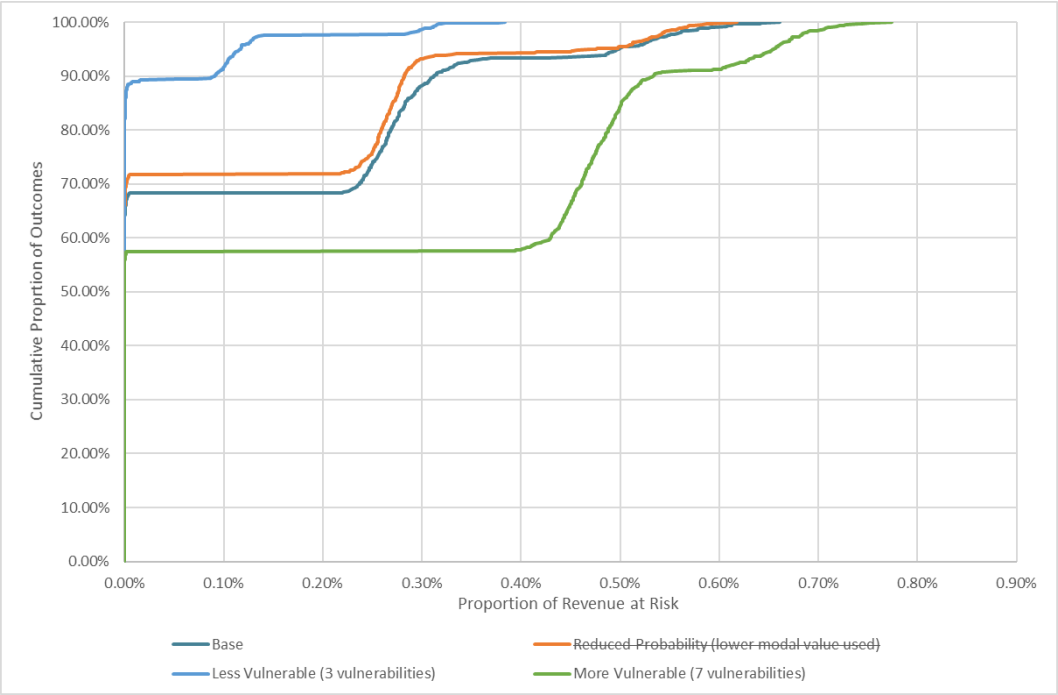


Figure 6-4 - Isolated Infection/Propagation Effect of Infection Probability changes

With this effect isolated, the impact of these parameters is more observable. Vertex vulnerability now has a clear bearing on the potential impact from incidents. With a 93% chance of infection and propagation, the occurrence of impacts in 7-vulnerability cases is not only more frequent, but also more damaging at 40bps of effective revenue.

An apparent oddity is the similarity of outcomes for the Base and Reduced Probability cases but, in this context, they are essentially the same and any difference is due to random noise. In order to focus on the outcomes of hacking incidents, the probability of an attempt was fixed at 100%, so the probability parameter would have no effect.

These runs therefore show that the hacking mechanisms in the model are working as expected. It also suggests a source for the anomalous results in Figure 6-3 may simply be the noise of random events. To test this, the contributions from each of the four categories for an isolated case are shown in Figure 6-5, though it is important to note that, due to the quantities of data output, these are from a separate instance of the model.

It should be noted that, despite the probability of a hack event occurring 100% of the time, the probability of a hack being successful is still predicated on successful versioning. Therefore, unless a new exploit has been found, the attack will be unsuccessful as the defender will have already been patched. Patching influence is what causes the apparent discrepancy between the actual proportion of successful hacks and the proportion forecast in Figure 5-7.

	Hacking	Failure	DOS	Insider
Average	0.00%	0.03%	0.01%	0.00%
Std. Dev	0.02%	0.01%	0.14%	0.02%
Min	0.00%	0.01%	0.00%	0.00%
P99.9	0.00%	0.01%	0.00%	0.00%
P99	0.00%	0.01%	0.00%	0.00%
P90	0.00%	0.01%	0.00%	0.00%
P80	0.00%	0.02%	0.00%	0.00%
P70	0.00%	0.02%	0.00%	0.00%
P60	0.00%	0.02%	0.00%	0.00%
P50	0.00%	0.03%	0.00%	0.00%
P40	0.00%	0.03%	0.00%	0.00%
P30	0.00%	0.04%	0.00%	0.00%
P20	0.00%	0.04%	0.00%	0.00%
P10	0.00%	0.05%	0.00%	0.00%
P01	0.00%	0.07%	0.00%	0.00%
P0.5	0.00%	0.07%	0.10%	0.00%
P0.1	0.25%	0.08%	2.31%	0.07%
Max	0.48%	0.08%	3.08%	0.48%

Figure 6-5 - Category impact by percentile of cases affected

As the data above shows, the majority of apparent impacts are caused by failures, but this is also a very low impact category, unable to cause the rare but disruptive impacts of the other categories. The costs attributable to the range of value of failures does coincide with that in which the anomalies occur, suggesting unexpected results encountered above are simply ancillary noise.

Hacking and Insider threats appear to be evenly matched in terms of both impact and likelihood, while DoS attacks represent a significant threat. This will be considered in the discussion.

6.2 Impact of Monoculture and "Hardening"

Once again, the results are mostly indistinguishable, with minor variation at the top percentile which again runs counter to expectations, with the results shown in Figure 6-6 up to the 99.5th percentile in keeping with the SCR.

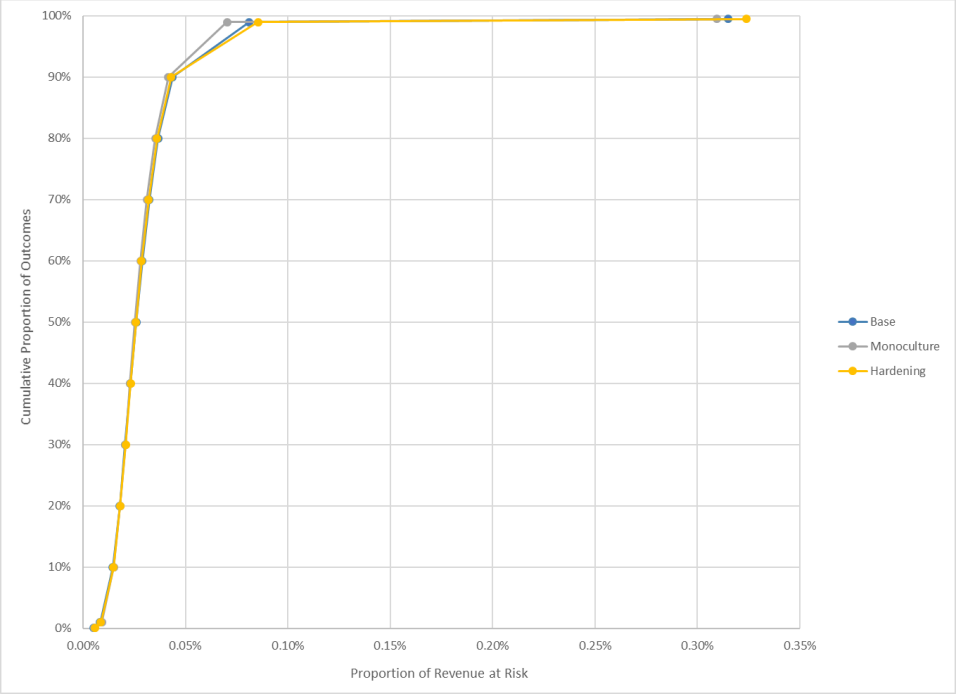


Figure 6-6 - Results from Sensitivity to Node Propagation Resistance Changes

Hardening of nodes would intuitively lead to preferential outcomes, yet it appears to incur higher losses than the Base case. Meanwhile monoculture, which this (and other) papers have noted is detrimental, appears to be preferable to the Base case. A detailed analysis of these variables with a focus only on cases where a hacking attempt occurs is presented in Figure 6-7.

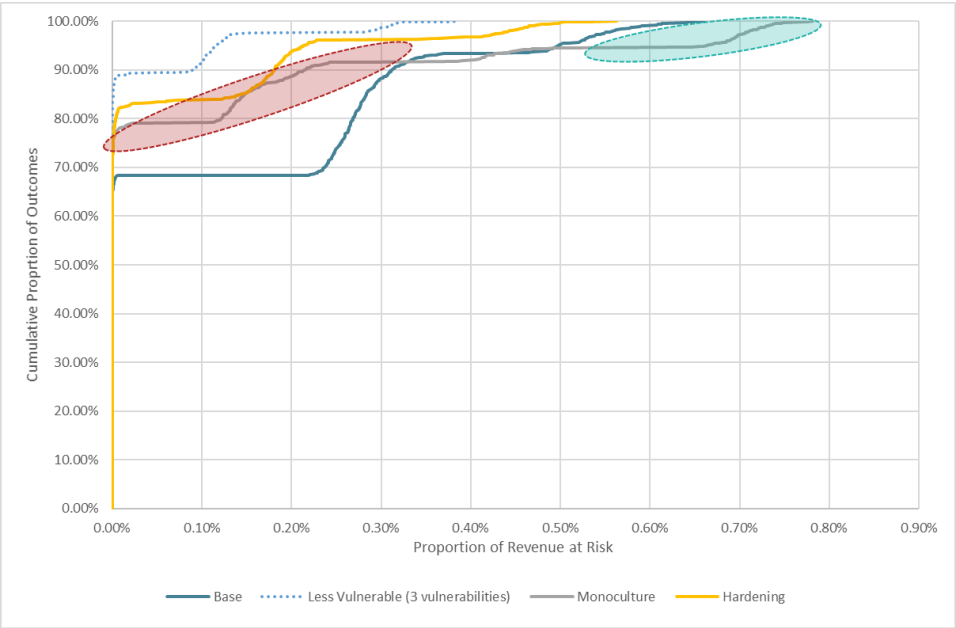


Figure 6-7 - Isolated Infection/Propagation Effect of Node Propagation Resistance Changes

The figures for hardening of nodes show how beneficial such measures can be, resulting in significant improvements to both likelihood and impact of incidents in comparison to the Base case. Material impacts are nearly 15% less likely to occur and when they do occur, reach a relative plateau at around two thirds of that in the Base.

Surprisingly monoculture appears to achieve improvements in impact likelihood approaching those seen from hardening (red shading), despite prior statements that monoculture is undesirable. This apparent improvement does, however, reverse itself at the 95% percentile (green shading), at which point it suddenly exceeds the losses exhibited in the Base case.

This behaviour may seem counterintuitive but there is a sound explanation. Unlike direct changes to vulnerability, the implementation of monocultures in SafetyNet effectively causes a dislocation between infection and propagation probabilities. When a hacking attempt occurs, a new Attacker is created with two random exploits and this is then applied to a randomly selected node and the probability of infection remains 78%.

However, with the vulnerabilities now fixed, propagation is now a binary event. Either one of the two exploits are the monoculture vulnerability (20% chance), or neither is (80% chance). If the monoculture is exploited, propagation will be catastrophic which accounts for the long tail. If neither of the Attacker's exploits is that of the monoculture, propagation likelihood falls as the pool of vulnerabilities from which the Attacker's vulnerabilities must match is one fewer. Consequently, instead of a 78% chance of propagation it is now only $\frac{4}{9} + \left(\frac{5}{9} * \frac{4}{8}\right) = 72.2\%$, per the formula in Figure 5-8, and it is this which causes the reduced impact in the red shading.

6.3 Impact of Graph Structure and Scale

Several cases are presented in Figure 6-8, showing how these changes to structure affect likelihood and impact of incidents. The Base and "High Base" cases are both included to show how the variation in results that can arise simply through randomness. Despite fundamental changes to the graph necessary to construct these cases, the high impact outcomes predominantly fall within the constraints of Base Case runs.

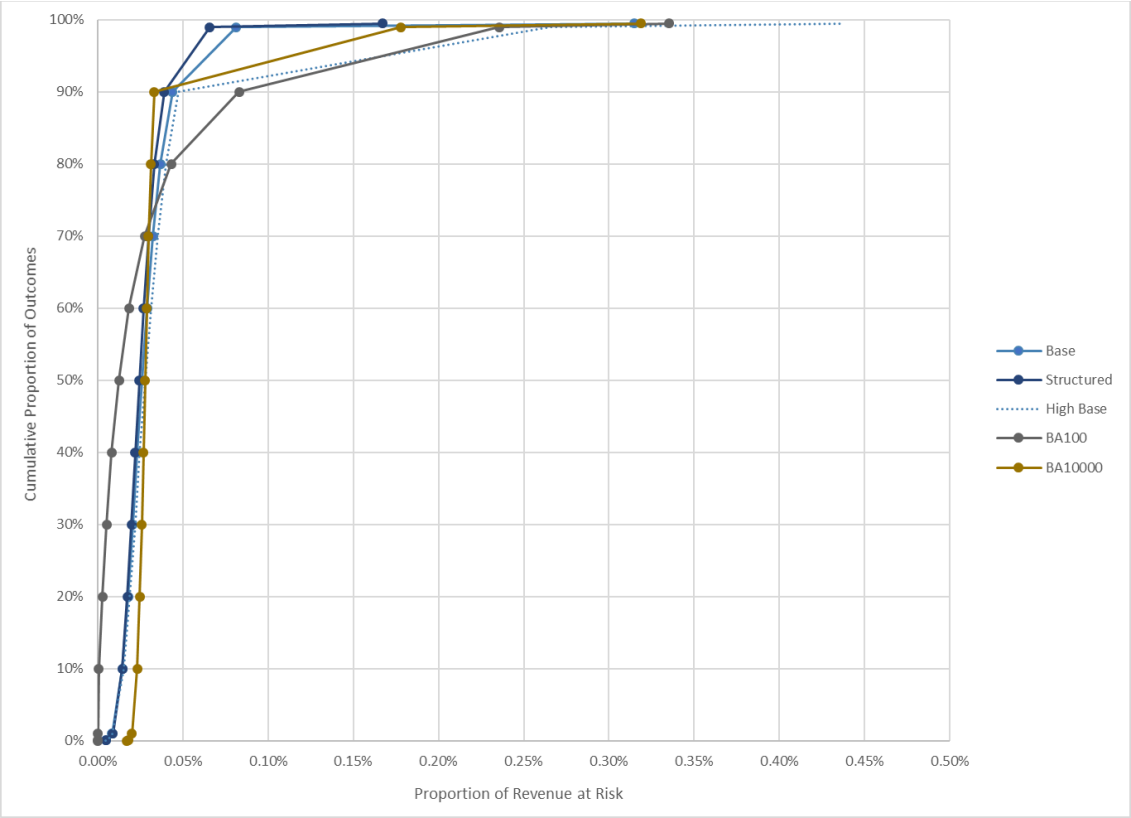


Figure 6-8 - Results from sensitivity to graph structure and scale

At lower probabilities, however, there is a noticeable difference between the revenue at risk of the 1000 node graphs, including the structured graph, when compared to the 100 and 10,000 node BA graphs. One noticeable detail is that there is zero impact in over 10% of outcomes in the 100 node BA graph.

To help better identify trends, these cases were once again run with a guaranteed chance of a hack occurring and all other sources of cost ignored. These results are shown in Figure 6-9.

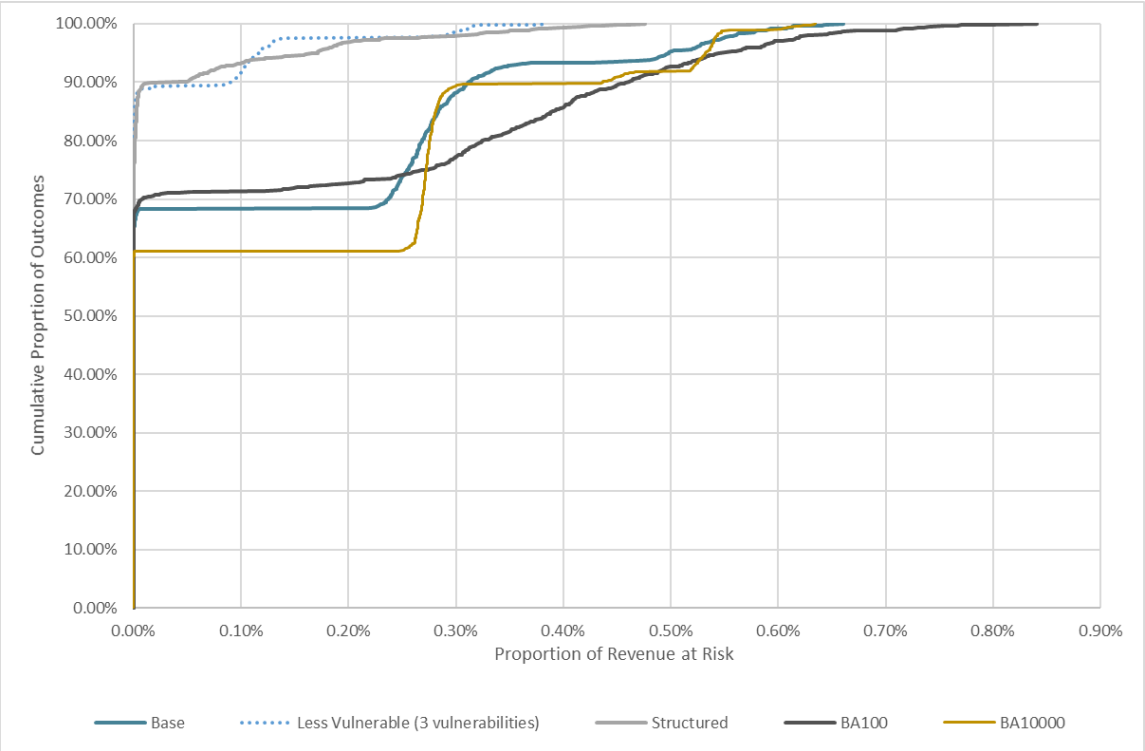


Figure 6-9 - Isolated Infection/Propagation Effect of Graph Structure and Scale changes

There are a couple of interesting outcomes in this set of results. The first is the low impact and likelihood demonstrated by the Structured graph. This is due to the low degree of individual nodes, with the tree like structure causing leaf nodes to have a connectivity of 1 and the graph as a whole to have a lower average degree. While low connectivity is beneficial for network robustness and failure resilience, it is a penalty when the threat relies on it for propagation.

The second is that, despite the order of magnitude change in scale with each case, the BA-based graphs follow a similar path. However, the surprise is that it is the larger scale graphs that give rise to the pronounced jumps in impact, instead of the expected behaviour that the larger numbers would smooth such changes.

6.4 Individual Vertex Value

Cat Bonds typically rely on a binary trigger, the closest proxy to which is the impact for a given node. This relationship between nodes and their contribution to the total impact is shown in Figure 6-10.

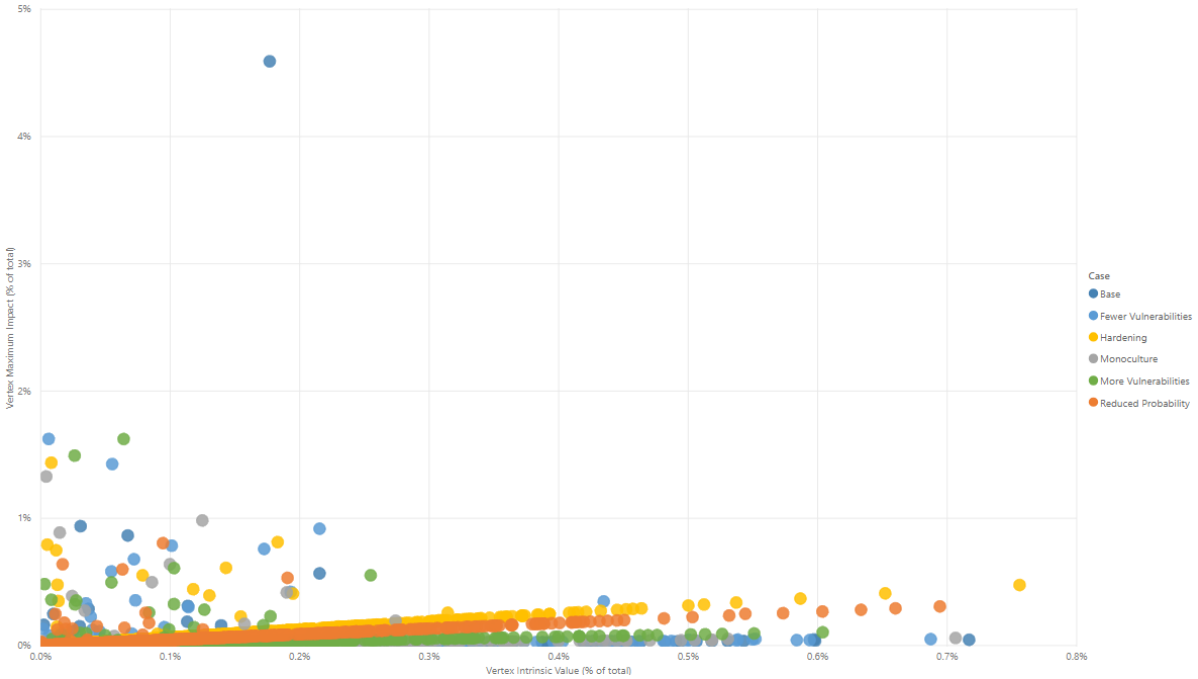


Figure 6-10 - Relationship between Node Value and its contribution to Total Impact

There are two tendencies represented above that arise because of the implementation of impacts in SafetyNet. Vertices falling on the very strong linear proportionality represent DOS attacks in which all vertices are compromised with the same percentage. While this percentage is typically low individually, the fact that all vertices are affected can lead to significant cumulative impacts.

Conversely, the widely scattered points indicating nodes that have been compromised individually but to a value greater than their individual contribution. Where this difference is small it may be due to a repeated hacking compromise, though this is extremely unlikely. Much more likely is a compromise as a result of an insider threat which may individually cause damage beyond the value of the node itself. Unfortunately, the originating incidents are infrequent and are essentially unpredictable with an R-squared of just 0.03.

7 Discussion

Based on the results from SafetyNet the distribution is comprised of two distinct elements. Traditional insurance would satisfy much of the distribution, with results well into the 99th percentile approximated by a lognormal distribution. However, the rarity and severity of outliers makes a strong case for the use of catastrophe insurance as these can have impacts well beyond the distribution itself.

Such a distinction would explain the Cover Limits currently in the marketplace that have proven to be of concern to Insureds, as mentioned in Section 3.2.1. It also implies that ILS/Cat Bonds may be used to address this deficiency, either as a standalone product to extend existing capped coverage or as an instrument available to Insurers for hedging of tail risk on uncapped policies.

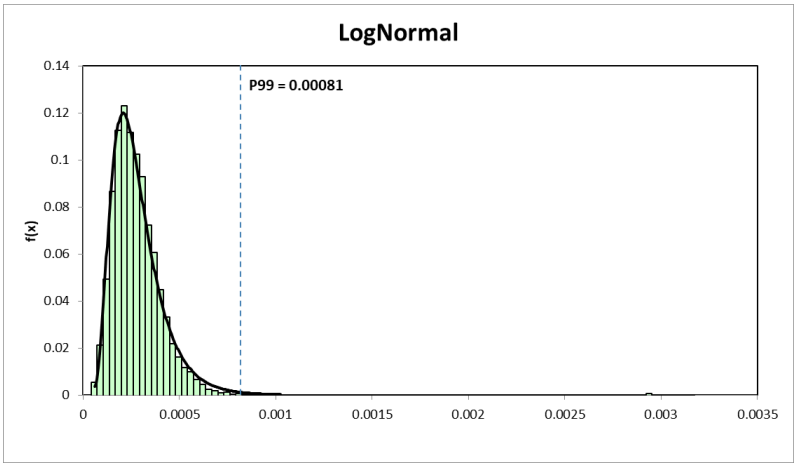


Figure 7-1 – Lognormal Distribution Fitting Curve for the Base Case, covering the bottom 99.5% of results

Before discussing these two purposes, the results suggest some model parameters may need refinements for future runs.

As noted in Section 6.1, the patching mechanism in place may need further refinement as it does appear to be causing some convolution. However, removing or replacing it is not trivial, as there is no information on which to substantiate an alternative. The removal of this mechanism would lead to a failure of all hacking attempts as there would be no way for exploits to supersede vulnerabilities.

Adjustment may also be necessary for impact from DoS attacks. While precedents exist for some extremely disruptive DoS attacks, such as the DynDNS outage (Red Button, 2016), or BGP attacks/mistakes (Toonk, 2017), these attacks are unlikely to affect the whole of an organisation simultaneously but rather regional activities may be affected. Consequently, the impact is likely to be overestimated SafetyNet and warrants revisions to the impact distribution or approach if a suitable data source were available. Alternatively, impact could be limited by defining a suitable subgraph – a particularly plausible approach if applied to real-world network data.

The uncommon nature of distributed attacks, combined with very skewed distributions, make extreme values even more so. Nevertheless, such outcomes can impact the mean and standard deviation, though as DoS valuations are an existing outlier, this change would tighten the distribution.

Certain behaviours would also be worth refining, such as those related to monoculture. While there are good reasons for the results as they stand, there are two aspects of the underlying assumption that could be reconsidered. The first is how a monoculture is incorporated into the vulnerabilities of a node as opposed to added. Alternate approaches may be used which would remove the subsequent propagation probability improvement observed. This mechanism of propagation does have significant potential for further study though.

The second, which may apply to other randomly generated values in SafetyNet, is whether they are random in the first place. As shown by (Albert, Jeong, & Barabási, 2000), directed attacks can be significantly more damaging than random ones. Opportunities for such attacks in SafetyNet include the selection of vulnerabilities an Attacker may choose to exploit, or the node they choose to target. Current approaches to Insider and DoS incident impact make targeting of attacks irrelevant, though incorporation of previous suggestions would enable such distinction in the future.

Any incorporation of targeting is likely to increase the magnitude of the associated event as the highest value or most vulnerable nodes would be the highest priority targets, resulting in greater single target value loss or total propagation losses. The probability would however remain unaffected.

Another aspect that bears further consideration is the graph structure. The use of BA graphs in SafetyNet was in part a function of their existing acceptance for internet modelling, and they may continue to be appropriate when modelling an inter-organisational network, such as an Insured portfolio and the associated supply chain. An intra-organisational network is much more structured though, and this can have a significant impact as shown in the comparison with the Base case.

This difference is also likely to be compounded by other common security countermeasures, such as network segmentation. A segmented network, represented by subgraphs connected by hardened nodes to limit propagation, is an unlikely occurrence in a BA graph with its higher connectivity and random connections, but much more readily constructed in a structured graph. Structuring would also be conducive to other behaviours, such as the identification of subgraphs for DoS attacks.

7.1 Applications to Catastrophe Bonds

As has become apparent when modelling the tail risk in SafetyNet, the infrequency of these events poses a significant challenge to evaluation. The infrequency can cause significant volatility when these rare events finally occur, and this can lead to difficulty in distinguishing between signal and noise in the data. Given this volatility, the question of how to determine what a "catastrophe" is remains.

It is also worth bearing in mind that the determination of a catastrophe is only relevant to the minimum threshold of a Cat Bond. The upper limit, on the other hand, is defined at the time of Cat Bond creation as the principal of the bond and any losses in excess of this will be uncovered.

7.1.1 A Catastrophe for the Insured – The Parametric Trigger

Before addressing how a Parametric Trigger could be constructed, the first step is determining what a catastrophe is. Defined as "one or more related losses whose consequences are extremely harsh in their severity…", one interpretation is that it is much like a default. If this is the case, in much the same way as a default, the financial stability of the organisation would have a bearing on what consequences the organisation would be capable of withstanding.

While financial metrics, particularly ratios to Revenue[12] (in order to make them relatable to model output), are simple and readily available, but this is somewhat missing the point. Such considerations are the raison d'être for the Credit Ratings agencies in the first place and they are thus well suited to determining the threshold at which such losses may be considered catastrophic. Thus, the information from Section 3.3 gains relevance as a means to associate the risk from a model such as SafetyNet with the financial stability determined in a Credit Rating, with the two linked together by the idiosyncratic value of a Revenue/Debt ratio.

Under this paradigm, the Insurer's model (in this case, SafetyNet) would determine the distribution of information security risk, while the Credit Rating provides an estimate of the organisation's financial surety on which the level of catastrophe is based. Thus, a financially stable organisation may not be threatened by the loss of large proportions of annual revenue, while a heavily indebted company may require only a small impairment to cause catastrophe. The case of Equifax and how the large headline figure relates to a seemingly minor credit impact is available in Appendix 10.5.

Further research is therefore needed to determine a suitable inverse relationship between the proportion of revenue that gave rise to a default, along with the credit rating. This relationship could then be used to forecast the proportion of revenue that constitutes a catastrophe, given the credit rating of the organisation.

With this suitable threshold for what constitutes a catastrophe, the assumption concerning distribution of value at risk across the graph can be revisited. Currently, this is assumed to be a single exponential distribution across all nodes, but it is clear from Figure 6-10 that there is

[12] Alternatives include:
Operating Cash Flow assumes surplus cash flow, after paying necessary expenses, is available to cover unexpected additional costs.
Free Cash Flow is as above, but after capital expenditure as well, though this may be deferrable if necessary.
Net Income includes non-cash charges, such as Depreciation & Amortisation, though in some cases this could be used as a proxy for maintenance capital expenditure.

insufficient relationship between impact and node value to identify high risk targets ex ante. This may not be a fair representation of reality, however, as it's possible that an organisation may have an extremely high concentration of value in a single node or location. If such concentrations are identifiable, it raises the possibility of a trigger based on a "cyber weathervane".

Such a service would effectively be a managed Intrusion Detection System (IDS), located on-path to catastrophic value concentrations. It would need to be administered by an independent third party in order to remain impartial in case of the inevitable disputes and should not affect the existing threat landscape, either through new vulnerabilities or controlling existing ones. Managed IDSs exist, but do not yet appear to be marketed for such purposes. If such approaches gained traction, the resultant fall in costs would likely be another positive externality to add to those in Section 3.2.3.

7.1.2 A Catastrophe for the Insurer – The Indemnity Trigger

In contrast to the complexities of the case above, a catastrophe to the Insurer is actually very simple to determine, both in terms of the value and the trigger. The value is determined by the Bond Sponsor (an Insurer) at the level of exposure at which they wish to hedge themselves, or are simply unable to provide coverage.

The trigger for such a bond is therefore equally simple. It is the point at which claims from the underlying policy exceed the level prescribed by the Insurer, and therefore functions for the Insurer in a very similar manner to that of a policy deductible for the Insured. If a $115mn Cat Bond is constructed on top of a $10mn catastrophe for the Insurer, underlying losses will be covered up to the value of $125mn, with the first $10mn covered by the Insurer and the subsequent $115mn covered by the Bond.

Complexity in this case therefore lies in the margin the Insurer chooses to keep, and the appetite for the resulting bond. An example, building upon the figures above, is presented in Appendix 10.6.

7.2 Opportunities for Model Development

In addition to the adjustments to existing parameters suggested previously, several opportunities for enhancement of the model have arisen. The first is through the refinement of valuation approaches in SafetyNet to better utilise existing frameworks.

The Kunreuther-Heal Model is frequently cited among literature for improving the accuracy of valuation estimates and originates from a paper by (Heal & Kunreuther, 2004). The model, originally intended for terrorism and based on Game Theory, recommends the deconvolution of values into component elements to better capture value ranges. SafetyNet does to some extent adopt this approach on the dimension of threat categorisation by using four categories, but there is further room for improvement.

By their very nature, Standards provide a good basis for adoption and in the theatre of cyber insurance one is currently under review. The upcoming ISO Standard 27102 (ISO, 2018) lays out four different categories of costs for which value could be ascribed; Business Interruption, Liability, Incident Response Costs and Legal and Regulatory Fines and Penalties. Adoption of these categories would help build a rationale for the impact distributions attributable to incident categories.

Along with revisions to impact categorisation, closer alignment with a threat framework such as that of ENISA may also be of benefit. While the coarser categorisation in SafetyNet was in part driven by the lack of data, in time this should improve. As it does, the use of more granular categorisation would help better delineate impacts and avoid the risk of double counting.

A second avenue for improvements lies not with the model itself, but with the inputs. As graphs can apply regardless of scale, the use of SafetyNet at portfolio level is also possible. At this level, nodes would represent businesses with their respective risks of infection and propagation. This level of detail has the added advantage that a rudimentary graph may be constructed through the use of publicly available information, such as Annual Reports, which detail key supplier/customer relationships.

Models at this level of resolution would allow for incorporation of risks such as supply chain compromise, as exhibited in the Target breach. It is also at this level that monoculture risks would become particularly interesting, with the potential to disrupt portfolio diversification.

At the macro end of the scale, it would also be possible to consider impacts at the AS level, incorporating real-world information which is available from (CAIDA, 2019). However, not only is this extremely resource-intensive due to the size of resulting graphs, but it's also likely to be too high level to be of interest to Insurers. Their abstract and cross-border nature would further hamper efforts to offer insurance at that level.

Another input improvement worthy of further work is the expansion of the adversarial behaviour to utilise applicable CVEs. This would not only be of interest but would also help justify data regarding vulnerability patching. However, the practical likelihood of obtaining such a detailed (not to mention sensitive) dataset outside of the proprietary environment to be modelled is very slim.

7.3 Opportunities for Further Research

As mentioned earlier in 7.1.1, a crucial next step to this line of research is to explore the relationship between past default events, the respective credit rating at the time and the impact to revenue that

precipitated the event. While seemingly straightforward, there are a multitude of idiosyncrasies involved that complicate this process. Suitable findings may unlock utility, not only within the insurance product itself, but also from existing financial instruments via the relationship.

The benefits within the realm of insurance would be the creation of parametrically triggered Cat Bonds, enabling Insurers to dissociate from the first tranche of risk. In turn, this would enable greater flexibility in the marketplace, with organisations able to source catastrophe insurance from a different provider or simply insure for catastrophe only. A potential disadvantage of this flexibility is in the commercial complexity, as splitting a claim between Insurers can be difficult.

Beyond insurance, the bridge to the financial markets this connection would provide may allow Insurers to hedge their tail-risk without needing to turn to indemnity-triggered Cat Bonds. Products such as Credit Default Swaps (CDS) already exist that allow investors to speculate on the financial stability of a company, allowing Insurers to invest in Capital Markets to hedge risk, instead of creating an ILS to allow Capital Market participants to invest in insurance. CDSs would also allow for scaling, with changes in coverage met by an increase or decrease in CDS holdings, whereas a Cat Bond is of fixed size once issued.

Not all areas identified for further research may yield improvements to the prospects for ILSs, however. One of their attractions is a perceived lack of correlation, or zero-beta, to other Asset Classes (Engman, 2002). This stands to reason for other catastrophes, as a hurricane is unlikely to be related to a recession, but due to the extensive human impact on Information Security, the same may not be true of ILS backed by cyber insurance. With some surveys suggesting over 5% of security professionals are “Grey Hats” (Osterman Research, 2018), or IT professionals who also participate in criminal activity, a loss of jobs may result in the transformation of Grey Hats to malicious Black Hats and a rise in cyber incidents. Unfortunately, data with which to inform such a hypothesis would require a recession!

8 Concluding Remarks

Through the course of this paper, a model has been developed that uses a more nuanced propagation mechanism than previous publications. This can lead to different behaviours than purely probability-based approaches previously used, as well as lending further support to recommended practices such as patching (reduced vulnerability case) and network segmentation (hardening case).

Furthermore, the context in which Credit Ratings may be applied to inform cyber insurance decision-making has been laid out. With further research, this avenue could be of great benefit to the cyber insurance industry, helping both Insurers and Insureds manage their risk more effectively. It may also provide a business opportunity for independent network asset monitoring, beyond the existing managed IDS model.

While the growth outlook for Cyber Insurance as a whole looks bright, the demand for Cat Bonds in the sector has yet to be tested, with no cyber catastrophe policies currently outstanding in the market (Artemis, 2019). Whether this is a sign of immaturity, unknown risks or potential correlation is not clear.

While there is much to learn from the connection between financial and cyber catastrophe, one aspect is lost in the abstraction – for all other perils covered by Catastrophe Bonds there is a striking connection to loss of life. One can only hope that remains a lesson that does not need to be learned.

9 Bibliography

Accenture Security. (2019). *The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study.* Traverse City, MI: Accenture.

Action Fraud (UK). (2018, July 19). *Number of computer misuse fraud offences reported in England and Wales.* Retrieved from Statista: https://www.statista.com/statistics/754008/computer-misuse-fraud-offences-england-wales/

Akamai Technologies; TechValidate; Applause, Inc. (2019, July 22). *Frequency of updating digital games according to gaming companies worldwide as of August 2016*. Retrieved from Statista Web site: https://www.statista.com/statistics/608976/digital-games-frequency-of-updating-gaming-companies-worldwide/

Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and Attack Tolerance of Complex Networks. *Nature*, 378-381.

Aon Inpoint. (2017, June). *Global Cyber Market Overview.* Retrieved from Aon Web site: https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Artemis. (2016, August 25). *Cyber the fastest growing peril, will require reinsurance and ILS capital.* Retrieved from Artemis Web site: https://www.artemis.bm/news/cyber-the-fastest-growing-peril-will-require-reinsurance-ils-capital/

Artemis. (2019, August 10). *Catastrophe Bonds % ILS Risk Capital Outstanding by Risk or Peril*. Retrieved from Artemis Web site: https://www.artemis.bm/dashboard/cat-bonds-ils-by-risk-or-peril/

Bandyopadhyay, T., & Mookerjee, V. (2017). A model to analyse the challenge of using Cyber Insurance. *Information Systems Frontiers*.

Beckett, V., & Booth, G. (2015). *Cyber cat model on the bench.* London: Reactions.

Beiner, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Working Papers on Risk Management and Insurance No. 151*.

Berliner, B. (1985). Large Risks and Limits of Insurability. *The Geneva Papers on Risk and Insurance*, 313-329.

BitSight. (2018). *BitSight Security Ratings.* Retrieved from BitSight Web site: https://cdn2.hubspot.net/hub/277648/file-2505376057.pdf

Bittner, D., & Harvey, J. (2019, May 9). The Cyberwire Podcast: Episode 840. Fulton, Maryland, United States of America. Retrieved from https://thecyberwire.com/podcasts/cw-podcasts-daily-2019-05-09.html

Bloomberg. (2019, June 20). Bloomberg Terminal. New York, New York, United States of America.

Böhme, R. (2005). Cyber-Insurance Revisited. *Conference Proceedings of the Workshop on the Economics of Information Security.* Boston: WEIS.

Böhme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards a Unifying Framework. *Conference Proceedings of the Workshop on the Economics of Information Security.* Boston: WEIS.

Brealey, R. A., Myers, S. C., & Allen, F. (2011). *Principles of Corporate Finance.* New York: McGraw Hill.

Brumaghin, E., & Mercer, W. (2016, July 11). *When Paying Out Doesn't Pay Off*. Retrieved from Talos Intelligence Web site: https://blog.talosintelligence.com/2016/07/ranscam.html?m=1

CA Technologies. (2019). *Insider Threat - 2018 Report.* San Jose, CA: Broadcom. Retrieved from https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

CAIDA. (2019, August 10). *Centre for Applied Internet Data Analysis*. Retrieved from Centre for Applied Internet Data Analysis Web site: http://www.caida.org/home/

Cambridge Centre for Risk Studies. (2016). *Cyber Insurance Exposure Data Schema v1.0.* Newark: RMS. Retrieved from https://static.rms.com/email/documents/rms_cyber_exposure_data_schema_jan2016.pdf

Capco. (2018). *Cyber Insurance Pricing.* London: The Capital Markets Company NV.

Cartwright, E., Hernandez-Castro, J., & Stepanova, A. (2018). To pay or not: Game theoretic models of Ransomware. *Conference Proceedings of the Workshop on the Economics of Information Security.* Innsbruck: WEIS.

Citywire. (2019, July 27). *Citywire Web site*. Retrieved from Company Factsheets: https://citywire.co.uk/funds_insider/

Dubner, S. J. (2018, October 10). *How to Optimise your Apology*. Retrieved from Freakonomics Web site: http://freakonomics.com/podcast/apologies/

Eling, M., & Zhu, J. (2018). Which Insurers Write Cyber Insurance? Evidence from the US Property and Casualty Insurance Industry. *Journal of Insurance Issues*, 22-56.

Engman, F. (2002). A Cat bond primer for Investors and Insurers. *Nordisk Forsikringstidsskrift (Scandinavian Insurance Quarterly)*, 221-226.

ENISA. (2016). *Cyber Insurance: Recent Advances, Good Practices and Challenges.* Heraklion: European Union Agency for Network and Information Security.

ENISA. (2019). *ENISA Threat Landscape Report 2018.* Heraklion: European Union Agency for Network and Information Security.

Equifax. (2018). *2018 Equifax Annual Report.* Atlanta, GA: Equifax.

Equifax. (2019, May 10). *Equifax Investor Relations Presentation - May 2019.* Retrieved from Equifax Web site: https://investor.equifax.com/~/media/Files/E/Equifax-IR/reports-and-presentations/events-and-presentation/investor-relations-presentation-may-2019.pdf

EU. (2016, October 12). *Quantitative Factors, Qualitative Factors and Benchmark.* Retrieved from Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R1799&from=en#d1e430-3-1

EuroFinance. (2017, July 13). *What's your cybersecurity rating? (You may have one you don't know about).* Retrieved from EuroFinance Web site (part of The Economist Group): https://www.eurofinance.com/news-publications/whats-your-cybersecurity-rating-you-may-have-one-you-dont-know-about/

European Banking Authority. (2019, 05 20). *EBA Final Draft ITS on ECAIs' Mapping.* Retrieved from European Banking Authority Regulation and Policy Web site: https://eba.europa.eu/regulation-and-policy/external-credit-assessment-institutions-ecai/mapping-under-crr

Fahrenwaldt, M. A., Weber, S., & Weske, K. (2018). Pricing of Cyber Insurance Contracts in a Network Model. *Astin Bulletin*, 1-44.

Fazzini, K. (2018, November 12). *Moody's is going to start building the risk of a business-ending hack into its credit ratings*. Retrieved from CNBC Markets Web site: https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html

Fazzini, K. (2019, May 22). *Equifax just became the first company to have its outlook downgraded for a cyber attack*. Retrieved from CNBC Web site: https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html

Federal Reserve Economic Data (FRED). (2019, August 13). *ICE BofAML US Corporate BBB Option-Adjusted Spread*. Retrieved from Federal Reserve Bank of St. Louis Web site: https://fred.stlouisfed.org/series/BAMLC0A4CBBB

Fenn, G., & Cid, C. (2017). Securitisation of Cyberinsurance Risk: An Introduction. *Unpublished*, 1-14.

FICO. (2018, August 28). *Scoring Cyber Risk: The FICO Enterprise Security Score.* Retrieved from FICO Blog Web site: https://www.fico.com/blogs/fraud-security/scoring-cyber-risk/

Fitch Ratings. (2016, March 21). *Fitch: Rapid Growth in Cyber Insurance Would Be Credit-Negative*. Retrieved from Thompson Reuters Web site: https://uk.reuters.com/article/idUKFit952109

Fitch Ratings. (2017, September 27). *Fitch: Cyber Insurance - A Growth Opportunity with Unique Risks*. Retrieved from Thompson Reuters Web site: https://www.reuters.com/article/fitch-cyber-insurance-a-growth-opportuni/fitch-cyber-insurance-a-growth-opportunity-with-unique-risks-idUSFit8jXTLc

Fitch Ratings. (2017, April 20). *Fitch: Cyber Risk Is a Growing Threat to Financial Institutions*. Retrieved from Thompson Reuters Web site: https://www.reuters.com/article/fitch-cyber-risk-is-a-growing-threat-to-idUSFit994598

Guidewire. (2018, June 12). *Guidewire Cyence Risk Analytics Datasheet.* Retrieved from Guidewire Cyence Risk Analytics: https://www.guidewire.com/sites/default/files/media/pdfs/Guidewire_Cyence_Risk_Analytics_data_sheet_en.pdf

Heal, G., & Kunreuther, H. (2004). *Interdependent Security: A General Model.* Cambridge, MA: National Bureau of Economic Research.

Hopkin, P. (2017). *Fundamentals of Risk Management.* London: Kogan Page.

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk.* Hoboken, NJ: John Wiley & Sons.

ICAEW. (2019, March 1). *National Cyber Security Skills Strategy.* Retrieved from Institute of Chartered Accountance for England and Wales: https://www.icaew.com/-

/media/corporate/files/technical/icaew-representations/2019/icaew-rep-30-19-national-cyber-security-skills-strategy.ashx

Insitute and Faculty of Actuaries. (2016). *Solvency II - Life Insurance.* London: Insitute and Faculty of Actuaries.

Insua, D. R., Couce-Vieira, A., & Musaraj, K. (2018). Some Risk Analysis Problems in Cyber Insurance Economics. *Estudios De Economia Aplicada*, 181-194.

ISO. (2018). ISO 27102. *Information Security Management - Guidelines for Cyber Insurance*. Geneva, Switzerland: ISO.

Johnson, B., Böhme, R., & Grossklags, J. (2011). Security Games with Market Insurance. *Lecture Notes on Computer Science*, 117-130.

Johnson, B., Laszka, A., & Grossklags, J. (2014). The Complexity of Estimating Systematic Risk in Networks. *IEEE 27th Computer Security Foundations Symposium* (pp. 325-336). IEEE.

Kahneman, D., & Tyversky, A. (2011). *Thinking Fast, and Slow.* St. Ives: Clays Ltd.

Kenneally, E. (2017). CyRiE - Cyber Risk Economics. *Conference Proceedings of the Workshop on the Economics of Information Security.* La Jolla, CA: Department of Homeland Security.

Kovacs, E. (2019, June 19). *AMCA Files for Bankruptcy Following Data Breach*. Retrieved from Security Week Web site: https://www.securityweek.com/amca-files-bankruptcy-following-data-breach

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2019, May 21). *DDoS attacks in Q1 2019.* Retrieved from SecureList Web site: https://securelist.com/ddos-report-q1-2019/90792/

Laszka, A., Johnson, B., Grosklags, J., & Feleghyazi, M. (2014). Estimating Systematic Risk in Real World Networks. *Financial Cryptography*.

Laszka, A., Panaousis, E., & Grossklags. (2018). Cyber-Insurance as a Signalling Game: Self-reporting and External Security Audits. *GameSec 2018*, 508-520.

Little, S. (2019, May 07). *John Lewis specialist home insurance now covers cybercrime - and could pay up if you fall victim to online fraud*. Retrieved from Moneywise website: https://www.moneywise.co.uk/news/2019-05-07/john-lewis-specialist-home-insurance-now-covers-cybercrime-and-could-pay-if-you-fall

Lloyd's. (2018). *Pocket Guide.* London: Lloyd's.

Mactavish. (2018). *Cyber Risk & Insurance Report.* London: Mactavish. Retrieved from https://mactavishgroup.com/wp-content/uploads/2018/11/Mactavish-Cyber-Risk-Insurance-Report-November-2018.pdf

Maersk. (2017, August 16). *A.P. Moller - Maersk improves underlying profit and grows revenue in first half of the year*. Retrieved from Maersk web site: https://www.maersk.com/news/2018/06/29/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year

Marvin, R. (2018, March). What is Cyber Insurance, and Do You Need It? *PC Magazine Digital Edition*. Retrieved from https://www.pcmag.com/feature/358453/what-is-cyber-insurance-and-should-you-get-it

Matthews, L. (2018, March 9). *Why You Should Never Pay a Ransomware Ransom*. Retrieved from Forbes Web site: https://www.forbes.com/sites/leemathews/2018/03/09/why-you-should-never-pay-a-ransomware-ransom/#53653cde1753

Modigliani, F., & Miller, M. (1958). The Cost of Capital, Corporation Finance and the Theory of Investment. *American Economic Review 48*, 261-297.

Moody's. (2018, September 20). *Moody's: As cyber threat intensifies for US utilities, government support remains key to credit profiles*. Retrieved from Moody's Investors Service Web site: https://www.moodys.com/research/Moodys-As-cyber-threat-intensifies-for-US-utilities-government-support--PBC_1142449

Mukhopadhyay, A., Chatterjee, S., Bagchi, K., Kirs, P., & Shukla, G. (2017). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*.

NetDiligence. (2018). *2018 Cyber Claims Study.* Gladwyne, PA: NetDiligence.

Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. *WEIS.* Cambridge, MA: WEIS.

Olyaei, S., Ambrose, C., & Wheatman, J. (2018). *Innovation Insight for Security Rating Services.* London: Gartner.

Osterman Research. (2018, August 8). *White Hat, Black Hat and the Emergence of the Gray Hat: The True Costs of Cybercrime.* Retrieved from MalwareBytes Web site: https://resources.malwarebytes.com/files/2018/08/USA-White-Hat-Black-Hat-and-the-Emergence-of-the-Gray-Hat-The-True-Costs-of-Cybercrime_Sponsored-by-Malwarebytes.pdf

Pal, R., Golubchik, & Psounis, K. (2011). Aegis: A Novel Cyber-Insurance Model. *Lecture Notes on Computer Science*, 131-150.

Panasonic. (2019, 07 22). Frequency of server failure based on the age of the server (per year). *Statista*. Statista Inc.

Payne, M. (2017). *An overview of the cyber insurance industry: Challenges for insurers and insureds in quantifying and mitigating cyber risk.* Egham: Royal Holloway.

Ponemon Institute. (2018). *2018 Cost of Insider Threats: Global.* Traverse City: Ponemon Institute LLC.

PWC. (2015). *Insurance 2020 & Beyond: Reaping the dividends of cyber resilience.* Retrieved from PWC Insurance Web site: https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

Red Button. (2016, October 21). *Dyn (DynDNS) DOS Attack.* Retrieved from Red Button Web site: https://www.red-button.net/blog/dyn-dyndns-ddos-attack/

RMS. (2008). A Guide to Catastrophe Modelling. *The Review - Worldwide Reinsurance*, pp. 2-23.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?* Santa Monica, CA: RAND.

Rosenbleuth, A., & Wiener, N. (1945, October). The Role of Models in Science. *Philosophy of Science*, pp. 316-321.

S&P Global. (2018, February 16). *S&P Global Ratings360 to include Cyber Risk Insights from Guidewire Software's Cyence Risk Analytics*. Retrieved from S&P Global Ratings Web site: https://www.spratings.com/documents/20184/544129/SP_GLOBAL_GUIDEWIRE/730a701f-000d-4a5a-b502-b1449a3d9d53

Schwartz, G., Shetty, N., & Walrand, J. (2010). Cyber-Insurance: Missing Market Driven by User Heterogeneity. *Conference Proceedings of the Workshop on the Economics of Information Security.* Arlington, VA: WEIS.

Shah, A., Dahake, S., & Haran, S. H. (2015). Valuing Data Security and Privacy using Cyber Insurance. *SIGCAS Computers & Society*, 38-41.

Somanchi, S., & Telang, R. (2017). Impact of Security Events on Customer Loyalty. *Conference Proceedings of the Workshop on the Economics of Information Security.* La Jolla, CA: WEIS.

Spanos, G., & Angelis, L. (2016). The Impact of Information Security events to the Stock Market: A systematic literature review. *Computers & Security*, 216-229.

Standard & Poors. (2019). *Annual Global Corporate Default and Rating Transition Study.* New York: S&P Global Ratings.

Stockopedia. (2019, July 27). *Stockopedia Company Factsheets*. Retrieved from Stockopedia Web site: https://www.stockopedia.com

Thomas, P., Bratvold, R., & Bickel, E. (2013). The Risk of using Risk Matrices. *SPE Economics and Management*, 56-66.

Tondel, I. A., Seehusen, F., Gjaere, E. A., & Moe, M. E. (2016). Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective. *Lecture Notes in Computer Science*, 175-190.

Toonk, A. (2017, December 12). *Popular Destinations Rerouted to Russia*. Retrieved from Cisco BGPMon: https://bgpmon.net/popular-destinations-rerouted-to-russia/

Tosh, D. K., Vakilinia, I., Shetty, S., Sengupta, S., Kamhoua, C. A., Njilla, L., & Kwiat, K. (2017). Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance. *Lecture Notes in Computer Science*, 519-532.

UK Home Office. (2019, July 19). *Number of hacking incidents of crime experienced by businesses in England and Wales in 2017, in selected industry sectors.* Retrieved from Statista Web site: https://www.statista.com/statistics/322529/hacking-incidents-experienced-by-businesses-by-industry-england-and-wales/

Unitrends. (2018). *Cloud Survey 2017 Result - 4 Hour Recovery Time Objectives are the New Norm.* Retrieved from Unitrends Web site: https://www.unitrends.com/landing/4-hour-recovery-time-objectives-new-norm

UpGuard. (2018, November 1). *Our New Cyber Risk Score: Cyber Security Rating.* Retrieved from UpGuard Web site: https://www.upguard.com/blog/cstar-to-csr

UpGuard. (2019, February 14). *BitSight vs. SecurityScorecard.* Retrieved from UpGuard Web site: https://www.upguard.com/articles/bitsight-vs-securityscorecard

Vazza, D., Kraemer, N., & Gurwitz, Z. (2019, March 26). *The Cost of a Notch.* Retrieved from S&P Global Ratings Web site: https://www.spglobal.com/en/research-insights/articles/the-cost-of-a-notch

Williams, G., Schulz, R. C., Tesher, D., & Hazell, L. (2015, June 9). *Cyber Risk and Corporate Credit*. Retrieved from Standard & Poors Ratings Services Web site: https://www.spratings.com/documents/20184/86990/SPCyberRiskAndCorporateCredit/1742ca0c-3528-4317-a30f-d2d317d0e8d5

Wolthusen, S. D. (2019, February 18). Unit 4 - Network and Internet Robustness. Egham, Surrey.

Wolthusen, S. D. (2019, February 18). Unit 5 - Critical Infrastructures and Dependencies. Egham, Surrey.

Woods, D., & Simpson, A. (2018). Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments. *Conference Proceedings of the Workshop on the Economics of Information Security.* Innsbruck: WEIS.

Xu, M., & Hua, L. (2017). *Cybersecurity Insurance: Modeling and Pricing.* Schaumburg, IL: Society of Actuaries.

10 Appendices

10.1 Source Listing for Historic and Forecast Data

Publication Date	Publisher	Title	Year to which Statistic Relates	Topic	Value	Cited source
June 2018	Woods, Simpson	Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments	2017	Insurance industry size	$2.5bn	PWC
June 2018	Woods, Simpson	Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments	2020	Insurance industry size	$7.5bn	PWC
June 2018	Woods, Simpson	Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments	2022	Insurance industry size	$14bn	Allied Market Research
January 2018	Fahrenwaldt, Weber, Weske	Pricing of Cyber Insurance Contracts in a Network model	2015	Worldwide losses due to cyber security	$400bn	Fortune
January 2015	Beiner et al	Insurability of Cyber Risk	2013	Average loss	$9.4mn	Ponemon institute
January 2015	Beiner et al	Insurability of Cyber Risk	2013	Worldwide economic impact (low)	$300bn to $1tn	McAffee
January 2015	Beiner et al	Insurability of Cyber Risk	2013	Worldwide economic impact (high)	$1tn	McAffee
January 2015	Beiner et al	Insurability of Cyber Risk	2013	US economic impact	$500mn	World Economic Forum
January 2015	Beiner et al	Insurability of Cyber Risk	2013	Continental Europe	$192mn	NAIC
January 2015	Beiner et al	Insurability of Cyber Risk	2018	Continental Europe	$1.1bn	
August 2018	Laszka, Grossklags et al	Cyber insurance as a signalling game	2014	Average loss	$600k to $1.15m for large businesses	ABI
August 2018	Laszka, Grossklags et al	Cyber insurance as a signalling game	2019	Worldwide losses due to cyber security	$2.1tn	Forbes
November 2017	Insua, Couce-Vieira and Musaraj	Some Risk analysis problems in cyber insurance economics	2016	Worldwide economic impact	$450bn	McAffee
September 2017	Romanosky, Ablon, Kuehn, Jones	Content Analysis of Cyber Insurance Policies	2012	US	Less than $1bn	RAND Corporation
September 2017	Romanosky, Ablon, Kuehn, Jones	Content Analysis of Cyber Insurance Policies	2020	Insurance industry size	$7.5bn	PWC
September 2017	Romanosky, Ablon, Kuehn, Jones	Content Analysis of Cyber Insurance Policies	2018	Insurance industry size	$5bn	PWC
September 2017	Romanosky, Ablon, Kuehn, Jones	Content Analysis of Cyber Insurance Policies	2020	Insurance industry size	$10bn	ABI
September 2017	Romanosky, Ablon, Kuehn, Jones	Content Analysis of Cyber Insurance Policies	2015	US cyber insurance premiums	$2bn	Insurance Information Institute
September 2017	Fitch	Statement	2017	Insurance industry size (low)	$2.5bn	Fitch
September 2017	Fitch	Statement	2017	Insurance industry size (high)	$3.5bn	Fitch
September 2017	Fitch	Statement	2027	Insurance industry size (low)	$15bn (6-8x over decade)	Fitch
September 2017	Fitch	Statement	2027	Insurance industry size (high)	$28bn (6-8x over decade)	Fitch
September 2019	RMS	Estimate	2017	NotPetya cost	$3bn	Insurance Journal
February 2019	Marketwatch	33.8% growth for Cyber Insurance Market Size to 2024	2024	Insurance industry size (global)	$16.7bn	MarketWatch
February 2019	Marketwatch	33.8% growth for Cyber Insurance Market Size to 2024	2019	Insurance industry size (global)	$2.92bn	MarketWatch
February 2019	Marketwatch	33.8% growth for Cyber Insurance Market Size to 2024	2016	North American proportion of global cyber insurance industry	0.89	MarketWatch
February 2019	Marketwatch	33.8% growth for Cyber Insurance Market Size to 2024	2016	Total direct premiums	$2.19bn	MarketWatch
May 2018	Orbis Research	Global Cyber Security Insurance Market 2018	2023	Cyber security insurance market	$17.55bn	Orbis Research
May 2018	Orbis Research	Global Cyber Security Insurance Market 2018	2017	Cyber security insurance market	$4.52bn	Orbis Research
May 2018	Orbis Research	Global Cyber Security Insurance Market 2018	2017	Average loss	$3.6mn	Orbis Research
June 2017	AON	Global Cyber Market Overview	2015	Insurance industry size (gross written premium)	$1.7bn	Aon
June 2017	AON	Global Cyber Market Overview	2016	Insurance industry size (gross written premium)	$2.3bn	Aon
June 2017	AON	Global Cyber Market Overview	2015	US standalone cyber market projection	$1.5bn	Aon
June 2017	AON	Global Cyber Market Overview	2016	US standalone cyber market projection	$2bn	Aon
June 2017	AON	Global Cyber Market Overview	2017	US standalone cyber market projection	$2.6bn	Aon
June 2017	AON	Global Cyber Market Overview	2018	US standalone cyber market projection	$3.3bn	Aon
June 2017	AON	Global Cyber Market Overview	2019	US standalone cyber market projection	$4.4bn	Aon
June 2017	AON	Global Cyber Market Overview	2020	US standalone cyber market projection	$5.6bn	Aon
July 2018	CyberInsure One	Stats	2017	Ransomware damages	$5bn	CyberInsure One
July 2018	CyberInsure One	Stats	2015	Ransomware damages	$325mn	CyberInsure One
July 2018	CyberInsure One	Stats	2015	Cybercrime damages	£3tn	CyberInsure One
July 2018	CyberInsure One	Stats	2021	Cybercrime damages	$6tn	CyberInsure One
July 2018	CyberInsure One	Stats	2015	Cyber Insurance market	$2.5bn	CyberInsure One
July 2018	CyberInsure One	Stats	2020	Cyber Insurance market	$7.5bn	CyberInsure One
July 2018	CyberInsure One	Stats	2016	Cyber insurance premiums written	$1.35bn	CyberInsure One

10.2 Parameter Distribution Diagrams

10.2.1 Server Failure Rates

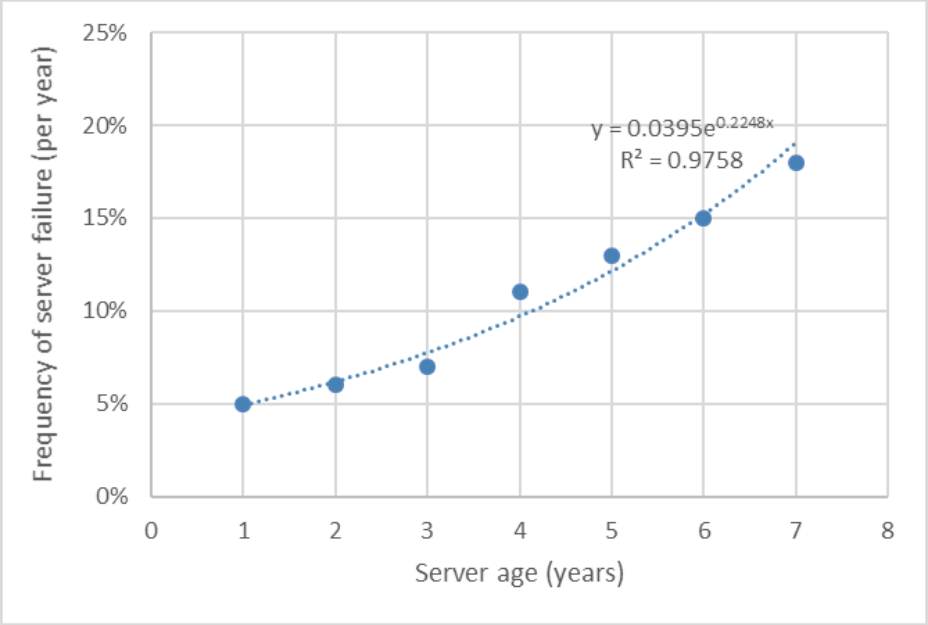


Figure 10-1 - Server Failure Rate Probability (Panasonic, 2019)

10.2.2 DoS Data – Distribution Fitting for DoS Downtime Durations

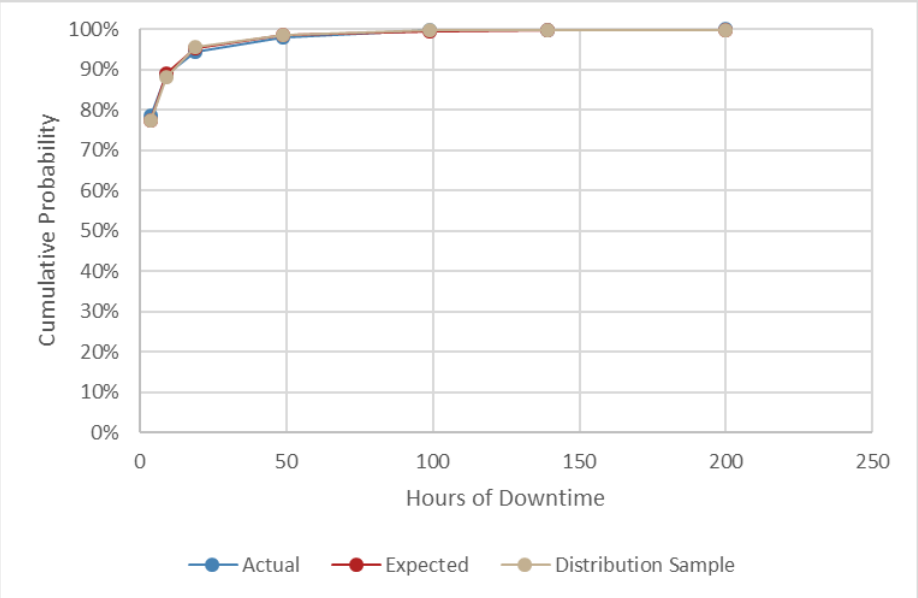


Figure 10-2 - DoS Downtime Distribution – Lognormal (0.1, 1.7)

10.2.3 Insider Threat Data – Ponemon Insider Threat Charts

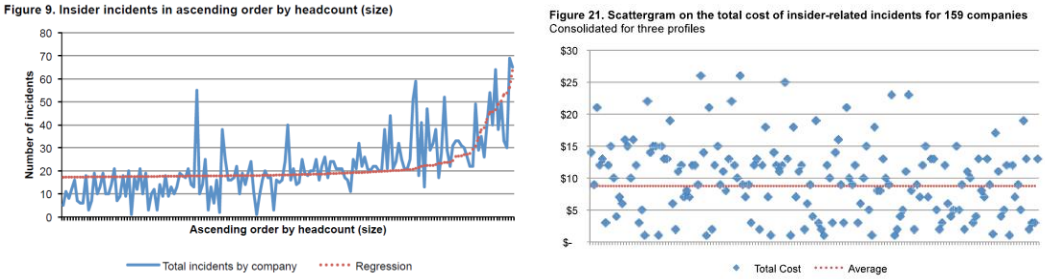


Figure 10-3 - Discrete x-axis charts. Source: (Ponemon Institute, 2018)

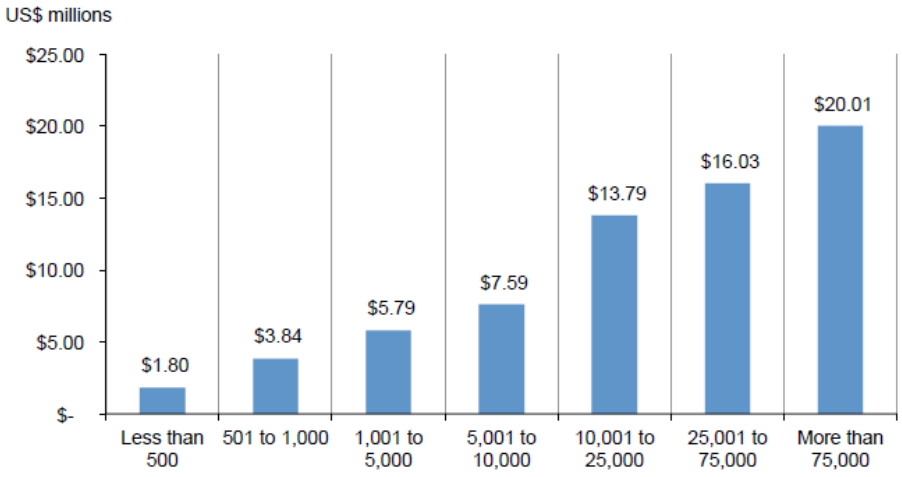


Figure 10-4 - Total annualised Insider Threat Cost by Global Headcount. Source: (Ponemon Institute, 2018).

10.2.4 Insider Threat Data – CA Technologies Event Frequency

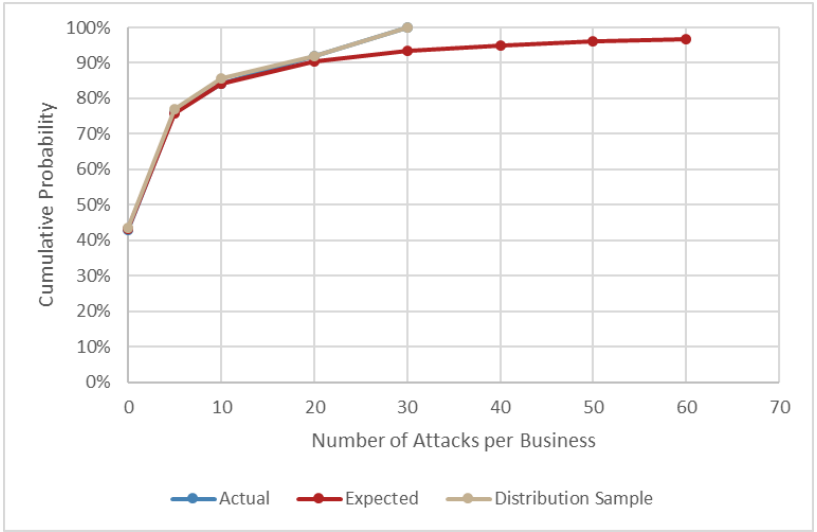


Figure 10-5 - Frequency of attacks per business. Source: (CA Technologies, 2019)

Note: Binning used in the CA Technologies report uses the category of >=30, so definition of the distribution tail is not possible.

10.3 SafetyNet Test Graph Diagram

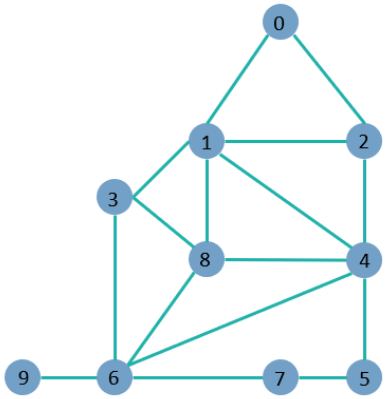


Figure 10-6 - Small-scale Test Graph used for SafetyNet unit tests

This Test graph was made to be simple, with a range of node degrees. Thus, some nodes are significantly more prone to disconnection than others (e.g. {9} compared to {1}).

10.4 Complete table of results

Description	Base	Reduced Probability	Monoculture	Hardening	Less Vulnerable	More Vulnerable	Structured	BA100	BA10000	High Base
	Per Section 5	Infection chance reduced to 1.2 incidents/year	All nodes share a vulnerability	Nodes with highest degree have only 1 vulnerability	Nodes have 3 vulnerabilities instead of 5	Nodes have 7 vulnerabilities instead of 5	Graph is generated using the algorithm in 5.3.4	Graph generated using Barabasi-Albert model, with 100 nodes	Graph generated using Barabasi-Albert model, with 10,000 nodes	Highest values using Base Case parameters out of 10 trials
Average	0.034%	0.041%	0.033%	0.042%	0.034%	0.034%	0.035%	0.033%	0.036%	0.040%
Std. Dev	0.127%	0.492%	0.142%	0.655%	0.162%	0.197%	0.410%	0.099%	0.173%	0.227%
Min	0.004%	0.004%	0.004%	0.005%	0.004%	0.004%	0.004%	0.000%	0.017%	0.004%
P99.9	0.005%	0.005%	0.006%	0.006%	0.005%	0.006%	0.005%	0.000%	0.018%	0.006%
P99	0.008%	0.008%	0.009%	0.009%	0.008%	0.009%	0.009%	0.000%	0.020%	0.009%
P90	0.015%	0.015%	0.015%	0.015%	0.014%	0.015%	0.014%	0.001%	0.023%	0.015%
P80	0.018%	0.019%	0.018%	0.018%	0.017%	0.018%	0.017%	0.003%	0.025%	0.019%
P70	0.021%	0.022%	0.021%	0.021%	0.020%	0.020%	0.020%	0.005%	0.026%	0.022%
P60	0.023%	0.025%	0.023%	0.023%	0.022%	0.022%	0.022%	0.008%	0.027%	0.025%
P50	0.026%	0.027%	0.025%	0.026%	0.025%	0.025%	0.024%	0.013%	0.028%	0.028%
P40	0.029%	0.031%	0.028%	0.029%	0.028%	0.027%	0.027%	0.018%	0.029%	0.031%
P30	0.032%	0.034%	0.031%	0.032%	0.031%	0.030%	0.030%	0.027%	0.030%	0.035%
P20	0.037%	0.039%	0.035%	0.036%	0.035%	0.034%	0.033%	0.043%	0.031%	0.040%
P10	0.044%	0.046%	0.042%	0.043%	0.042%	0.040%	0.039%	0.083%	0.033%	0.047%
P01	0.081%	0.075%	0.070%	0.085%	0.073%	0.202%	0.066%	0.236%	0.178%	0.266%
P0.5	0.315%	0.170%	0.310%	0.324%	0.173%	0.496%	0.167%	0.335%	0.319%	0.436%
P0.1	1.518%	2.297%	1.154%	1.847%	1.627%	1.338%	1.776%	1.543%	1.443%	1.780%
Max	6.369%	44.314%	8.432%	62.930%	7.303%	17.225%	39.126%	3.608%	11.829%	12.797%

Figure 10-7 - Complete table of primary results

10.5 Equifax – Relationship between Cyber Costs and Credit Rating

The relationship between a $1.35bn cyber cost headline and a paltry 40bps adjustment to the Credit Rating deserves further explanation. While reported cyber security costs since the incident is $1.35bn, or nearly 40% of 2018 revenue, the breakdown of figures beneath the headline are less concerning.

Of this $1.35bn, $417mn has effectively been investment in technology, providing ongoing benefits, rather than incident costs. A further $690mn has been accrued for legal costs and claims, but this sum has not been paid yet, but rather has been set aside in case it is. The fate of this money is ultimately pending legal outcomes and may be connected to the negative outlook. Meanwhile of the remaining $245mn, $125mn was covered by insurance and has been reclaimed, leaving only $120mn of direct cost exposure for investigations and consumer protection measures, paid out over the course of 3 years.

10.6 Example Indemnity Trigger Cat Bond

In this case study, using the results of the Base Case from SafetyNet, a company with $3.2bn in annual revenue seeks insurance coverage of $125mn, or just under 4% of revenues. As the losses are capped, this cap is incorporated into the distribution that arose in Figure 6-2 and a modified version is shown below.

With this cap in place, the mean falls to 0.034% and standard deviation is 0.11%. If the Insurer uses a Safety Loading of 2, this means that the company will pay premiums of 0.25% of their revenues, or $8.2mn per year in exchange for the $125mn coverage.

The Insurer chooses to accept up to a 1-in-250-year event, or the P99.5 percentile which is just over $10mn, or 0.3% of revenue. Based on this sub-distribution, with a mean of 0.029% with a σ of 0.019%, the Insurer would keep $2.1mn in premiums while passing the remainder, $6.1mn, onto the SPV of the Cat Bond.

The Cat Bond SPV on the other hand now holds the liability of risks falling between $10mn and $125mn, requiring $115mn of capital to back this liability. This money is raised on the capital markets from investors willing to receive a payment of $6.1mn in exchange for lending $115mn to the SPV for collateral. This exchange equates to a coupon of 5.3% with an expected chance of loss of less than 1 in 250 years.

While these numbers may seem arbitrary, they have been chosen as they resemble the revenue and cyber insurance coverage figures disclosed in Equifax' 2018 Annual Report. This means they can be contrasted to Equifax' debt. Thus, the Cat Bond effectively allows an investor to receive an effective coupon of 5.3% from a company that most recently issued debt with a coupon of only 3.6%. The risk of catastrophe is expected to be less than once in 250 years, while a default event on the debt for BBB-rated Equifax is only 1 in 100.

As noted by (Engman, 2002), the Bond may also be tranched, allowing for the most at-risk tranches to receive a larger coupon while the lower risk tranches receive a reduced coupon. Such a structure is very similar to those in use in Collateralised Debt Obligations.