Distribution Analysis for Information Risk (DAIR)

A Cyber Quantification Framework

GLOBAL RISK INSTITUTE AUTHORS:
Lois Tullo, Serguei Zernov

BANKINGBOOK ANALYTICS AUTHORS:
Sohail Farooq, David Gong

ABSTRACT

We know that cyber threats continue to evolve and pose increasingly significant risks to organizations.

We also know that the impact of cyber-attacks extends beyond direct financial consequences. Cyber incidents can lead to serious service disruptions, reputational damage and share price deterioration, along with potential for fines and litigation.

It's difficult to measure cyber risk in a systematic way and, as such, it's a challenge to monitor and manage from a risk capacity perspective.

To address this challenge, we have developed the **Distribution Analysis for Information Risk (DAIR)** framework. DAIR is a cyber quantification methodology that maps cyber events with a hierarchical risk taxonomy to evaluate operational, business and systemic risk economic capital.

DAIR will help organizations quantify cyber risk in a consistent and meaningful way, giving consideration to asset vulnerabilities as well as business and systemic considerations. In turn, DAIR can:

- Enhance a firm's understanding of cyber risk exposure by highlighting where the highest dollar level of threat may be coming from;
- Help management and boards set and monitor their cyber risk appetite, and make decisions based on the organization's capacity, appetite, and actual risk level;
- Better inform decisions relating to expenditures on cyber risk mitigation, economic capital allocation and insurance; and
- Help management demonstrate to regulators that they are managing cyber risk in a comprehensive way.

By embracing the DAIR approach, CROs and CISOs can add value by enhancing the firm's overall understanding and management of this important area of risk.

1. EXECUTIVE SUMMARY

The technology behind information systems evolves at an exponential rate. This brings with it an implicit rise in the complexity of systems as well as inevitability of cyber-attacks. The cost of cyber breaches is estimated to rise from $3 trillion in 2015 to $6 trillion annually by 2021[1]. Global spending on defending cybersecurity products and services is projected to exceed $1 trillion from 2017 to 2021[2].

A 21st century threat landscape is defined by cross-border threat agents, with threat trends that include substantial increases in software subversion by proliferating attacks on software-update supply chains, and the targeting of critically important systemic assets. Understanding the sources, targets and impact of cyber-attacks can help us develop better controls. However, the evidence of risk incidents relating to the cyber eco-system calls into question the effectiveness of internal control frameworks. Stakeholders' demand for greater risk transparency requires a shift from a pre-dominantly controls-based approach to one based on risk quantification, aggregation of loss estimates and recalibration of prevention strategies. Cyber risk forecasting and estimation now tops the priority list for businesses and governments.

While cyber breaches cannot be eliminated entirely, they can be averted by developing multiple approaches to improve the chances of mitigation. This paper presents Distribution Analysis of Information Risk (DAIR), a cyber risk modelling framework developed jointly by Global Risk Institute (GRI) and BankingBook Analytics[3] (BBA). The key contribution of DAIR is twofold. Firstly, it consolidates cyber risk into a single, organization-wide risk taxonomy and, secondly, it quantifies the cyber loss estimates using modelling approaches that overcome the data paucity challenge.

[1] [Herjavec Group, 2019]
[2] [Cyber Security Ventures, 2019]
[3] BBA (BankingBook Analytics) is a Toronto-based FinTech provider, focused on providing risk, finance and compliance consulting and microservices to financial institutions. For more information, please visit: https://bba.to

By aligning taxonomy and measurement, inconsistencies in risk assessment and reporting can be avoided. Preventive measures and mitigating controls can then be recrafted or recalibrated by analyzing the estimates of unexpected losses and the secondary harms that can result.

Cyber-attacks are not always comparable nor are the institutional risk thresholds. DAIR provides an 'apples to apples' measure relevant across different types of businesses, geographies and accounting systems.

Finally, the objective of developing DAIR is not so much to assign a hard dollar figure to cyber risk, but rather to view the risk contribution of losses due to cyber-attacks through the broader lens of other non-financial risks (NFR).

DAIR is particularly useful for financial services organizations, including, financial conglomerates, multinational and smaller financial institutions.

The rest of this paper is organized as follows: In section 2, we define cyber risk and develop an approach to consolidate cyber risk into non-financial and external market risks' taxonomy; sections 3, 4 and 5 provide coverage of the modelling framework; section 6 discusses insurability of the cyber risk, which is followed by our conclusion and suggested next steps. Appendix I provides an overview of existing cyber risk assessment approaches in Canada and the United States.

2. TAXONOMY OF CYBER RISK

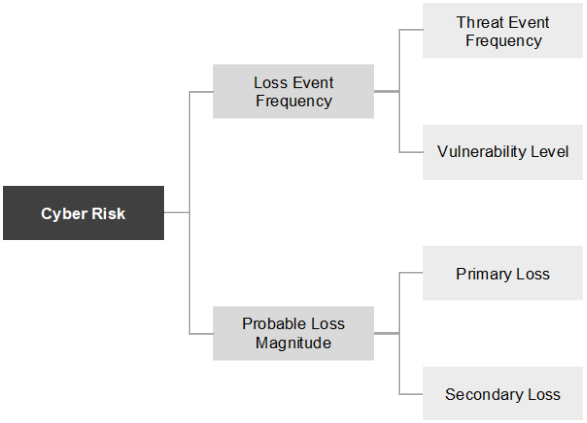
Cyber risk is inherent to running a business. As the cyber dependency trend increases, so does the risk of cyber-attacks, creating demand for new controls or defense mechanisms.

The term "cyber" is short for the word cyberspace[4], which is generally understood as the interactive domain composed of all digital networks used to store, modify and communicate information. It includes all information systems that support business, infrastructure, services and functional capabilities.

2.1. Risk classification and identification

In 2009, The Open Group[5] and FAIR[6] introduced definitions and taxonomy for information security risk. The following graphic illustrates how FAIR[7] decomposes the cyber risk.

Figure 1: Decomposition of cyber risk by FAIR[8]



FAIR Institute's framework distributes losses attributed to cyber into primary and secondary loss factors. Primary loss factors are mainly value/liability and volume losses associated with assets. Secondary loss factors are those organizational and external characteristics of the environment that influence the nature and degree of loss.

From a functional perspective, cyber risk is within the functional domain of information security. From a regulatory reporting perspective, cyber risk is classified as part of operational risk. Cyber risk's classification as operational risk[9] is mainly due to the similar consequences of both risk types.

Drawing from FAIR's factors-based definition of cyber and based on the current practice of managing non-financial risks, we are able to align the key variants of cyber incidents with broader organization-wide taxonomy:

Table 1 shows the variants of cyber loss factors and meta-risk classification. Large organizations would adopt all three of the loss distributions, while smaller organizations may only apply one or two of the distributions.

Figure 2 refers to the forms of losses developed by FAIR and maps them to the broader risk classifications:

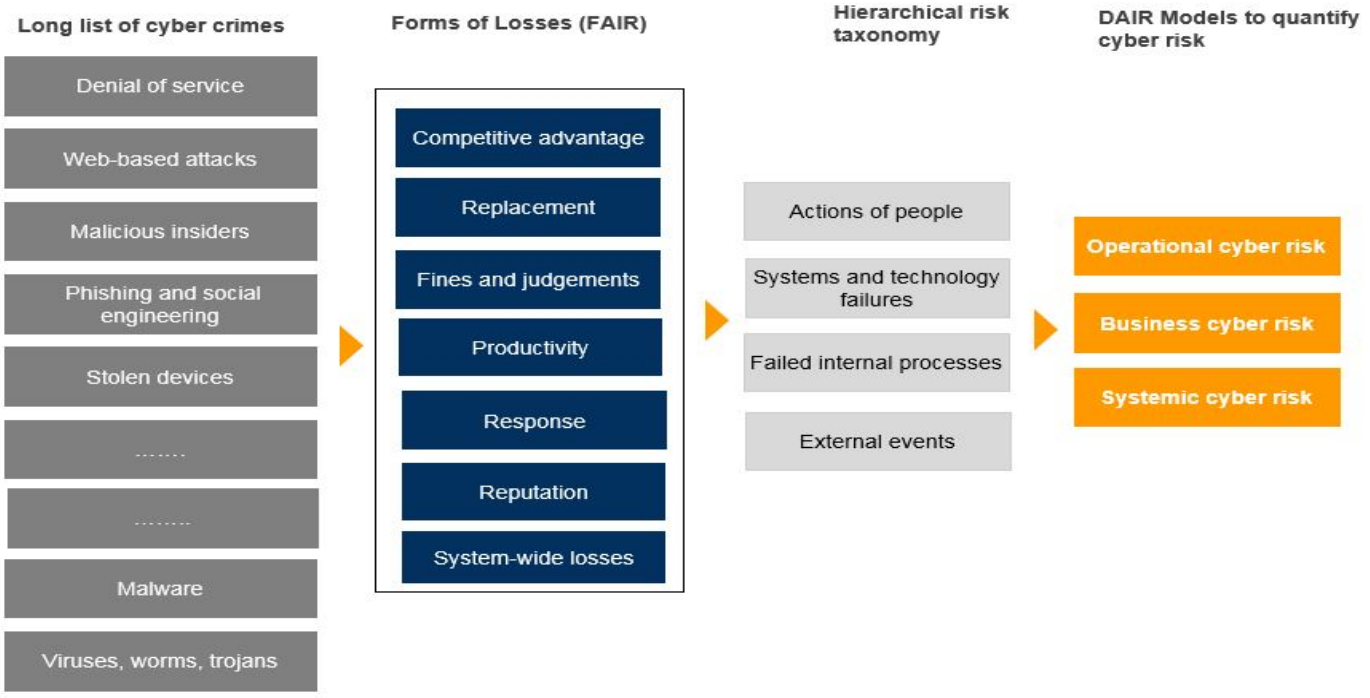
[4] [Biener 2015]
[5] The Open Group is an industry consortium that seeks to "enable the achievement of business objectives" by developing "open, vendor-neutral technology standards and certifications". Source: https://en.wikipedia.org/wiki/The_Open_Group
[6] Factor analysis of information risk (FAIR) is a taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of data loss events. It is not a methodology for performing an enterprise (or individual) risk assessment. Source: https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk
[7] [Jones 2009], [Technical Standard 2009]
FAIR framework is primarily concerned with "establishing accurate probabilities for the frequency and magnitude of loss events.
[8] Note that this diagram is not comprehensive, as deeper layers of abstraction exist that are not shown. Appendix 2 provides the definition for each term
[9] [Accenture/Chartis 2016]
Source: http://www.risktech-forum.com/research/accenture-chartis-the-convergence-of-operational-risk-and-cyber-security

From risk management's perspective, the design of a holistic modelling framework must encompass the impact of cyber losses across the entire cross-section of risks, as shown. The sections that follow describe these modelling approaches.

Table 1: Variants of cyber loss factors and meta-risk classification

Key Variants of Cyber Loss Factors	Organization-Wide Classification
Loss of cyber and/or physical property due to a cyber event	• Operational risk: Within the context of operational risk, cyber risk can be defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems". Basel's definition of operational risk includes legal risk, but excludes strategic and reputational risk[10]
Loss of reputation and/or damage to stakeholders' perception of an institution's franchise due to a cyber event	• Business risk: Business risk is the risk of having costs higher than revenues due to shocks to margins, volumes or costs
Loss of cyber and/or physical property due to contagion or systemic event caused by a cyber event, e.g., breakdown of international governance, cyber warfare	• Systemic risk: Systemic risk is the risk of disruption to financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the potential to have serious negative consequences for the real economy. Fundamental to the definition is the notion of negative externalities from a disruption or failure in a financial institution, market or instrument[11]

Figure 2: FAIR Institute's forms of losses mapped to institutional risk taxonomy[12]



.

[10] [BIS 2006]
[11] [Bank of England 2019]
[12] Note that reputational risk is excluded when operational risk is considered; see, e.g., BIS (2006), and is classified as business risk. Please see Appendix 2 for the definition of forms of losses which are based on Technical Standard [2009]

3. OPERATIONAL CYBER RISK QUANTIFICATION

Regulated financial institutions hold cyber risk capital as an implicit allowance within operational risk capital charge. Given the growing frequency and size of cyber-risk incidents, the contribution of cyber risk capital charge, within the operational risk capital, needs to be better understood.

Operational risk losses are typically driven by high-frequency, low-impact and low-frequency, high-impact events, constituting the body and tail of the distributions. These are referred to as, respectively, expected losses[13] and unexpected losses. Operational risk quantification involves probabilistic modelling of the frequency and impact of cyber-attacks. The losses can be interpreted from the probability distribution curve derived from the convolution process.

In practice, the body and the tail of data do not necessarily belong to the same, underlying, distribution or even to distributions belonging to the same family. For example, if we want to estimate probabilities associated with events that we have not seen, or have only seen rarely, an understanding of the tail of the distribution is particularly valuable. Extreme Value Theory appears to be a useful, inferential instrument with which to investigate the large losses. This is attributed to its double property of focusing the analysis only on the tail area (hence reducing the disturbance effect of the small/medium-sized data) and treating the large unexpected losses.

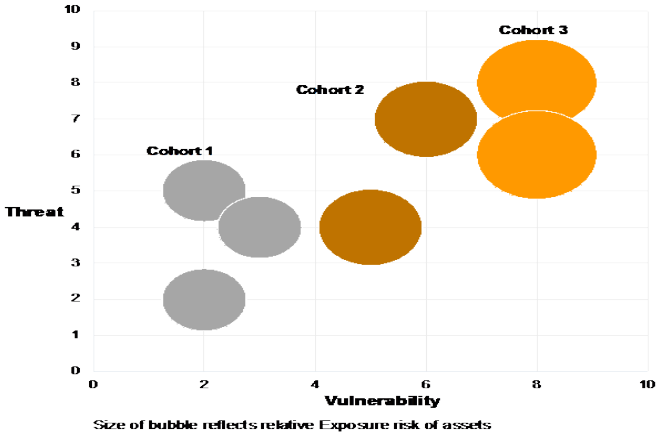
The steps noted below provide an overview of the practitioner's approach to developing estimates of operational cyber risk:

3.1. Step 1: Asset bucketing

Using vulnerability and threat as variables, we start by developing an exposure index to rank the most crucial assets exposed to cyber risk.

In an expert-led workshop, organizations can explore exposure scenarios; unattended vulnerabilities of IT systems[14] and portability of threats. Using an indexation approach, a ranking of most crucial assets exposed to cyber threats can be developed. This is shown [figure 3], drawn from a recent pilot project on cyber risk quantification.

Figure 3: Exposure indexation of crucial assets



The asset list may include digital and physical assets, critical data, operational services, IT systems and key members of the staff that can be damaged or destroyed. Assets can be indexed based on relevance and materiality and not on the basis of dollar value alone.

3.2. Step 2: Scenario Analysis

The process of scenario analysis involves determining the annual frequency of losses in excess of the threshold loss value limit. Each potential loss event can be defined as a scenario. Appropriately cleaned external loss data[15] is particularly useful for the identification of scenarios and the related parameterization of high-severity losses, especially as internal loss data is likely to be sparse. Scenario analysis is typically conducted in workshops involving specialists. These workshops are designed to discover the potential effects of exceptional but plausible events.

3.3. Step 3: Frequency distribution

The frequency distribution provides the distribution of the number of events over a time horizon, in this case one year. Given limited data and the novelty of cyber-attacks, institutions are likely to have too few frequency data points to use curve-fitting techniques. For example, if an institution had 2 years of cyber losses data, and the estimation horizon was 1 year, even if they had 1,000 individual loss events, the institution would still only have 2 frequency data points – the number of events in year 1 and the number of events in year 2. This problem is exacerbated for the 'tail' buckets, because typically low frequency-high severity losses would be non-existent.

[13] Expected losses attributed to cyber events can be described as the "usual" or average losses that an institution incurs in its natural course of business, for example, denial of service due to the server breakdown. Risk managers, regulators and financial supervisors are mainly concerned with the modelling of unexpected losses attributed to cyber events

[14] Example: Software-update supply chain

[15] Example RMS Cyber Loss Experience Database (CLED), launch of ORX Cyber risk initiative, Statistics Canada – The Canadian Survey of Cyber-Security and Cyber-Crime. As well as private security firm databases such as Fireye, Symantec, Blackberry, Proofpoint, Fortinet, McAfee, Rapid7, Synack, Crowdstrike, Digital Defense Inc, etc.

Using scenario analysis, we can avoid the data paucity challenge. In selecting a frequency distribution for operational cyber risk, we assume that:

- Cyber events are independent of each other.
- Availability of data is limited, often on an aggregate basis (arrival times) for varied cyber breaches.

The Poisson distribution is the industry standard for frequency modelling[16], and has been adopted within the model[17]. The Poisson distribution is easy to parameterize because it depends on one parameter only. This parameter is the shape parameter, λ (lambda), which indicates the mean number of events in the given time interval.

The formula for the Poisson probability density function is:

$$P_\lambda(x) = \frac{e^{-\lambda}\lambda^x}{x!} \quad \text{For } x = 0, 1, 2 \ldots$$

From a theoretical point of view, the Poisson distribution is defined as the probability of obtaining exactly *x* successes in *N* trials for a 'Poisson process'[18], and is given by the limit of a binomial distribution as *N* goes to infinity.

3.4. Step 4: Severity distribution

On the severity side, there is a great choice of distributions, although they are all skewed to the right and long-tailed. It is commonly agreed, and also borne out by empirical data that the Generalized Pareto Distribution (GPD) is preferred because among the three-parameter distribution choices, it is the simplest to fit[19]. Other choices include Weibull, Gamma, Lognormal and Loglogistic. The choice of severity curve has an influence on estimated loss numbers as long as one of these distributions is compatible with the data (as the distributions are quite similar). The general principle is to estimate the shape and scale parameters from the data and then use one of these to estimate the probability of interest.

However, precisely because the distributions are quite similar, the sensitivity of estimated losses to the choice of severity curve need not be large. One way of mitigating the importance of the choice of severity curve is, therefore, to ensure that the 'tail' anchor point for the severity curve is sufficiently far out in the 'tail', e.g. at the 95th percentile or above. This is achieved by choosing the threshold level, discussed below:

3.4.1. Choosing a threshold level

The idea is to approximate the distribution of losses above a certain threshold level, *u*. In order to make *u* reasonably large so that the Extreme Value Theory would apply, we need to estimate the parameters of the GPD[20] from the data that occur above the threshold level. We must ensure that there are enough data points to do this. It is not so hard to choose a reasonable value of the threshold given a large data set, but it can be difficult if the data set is small.

For any threshold value *v*, we look at the average amount by which the data points exceed this threshold, averaging just over the data points larger than *v*. The sample mean excess is an estimate of the true value, if the excess distribution is GPD, $G_{\xi,\beta}$:

$$\frac{\beta}{(1-\xi)}$$

where, β (beta) is a scaling constant and ξ (xi) captures the shape of GPD. The parameters ξ and β of the GPD (together with their confidence intervals) can be estimated using the maximum likelihood method.

3.5. Step 5: Convolution process[21]

The purpose of using convolution is to obtain a loss distribution curve that clearly states the estimate of losses. Convolution combines the frequency and the magnitude of losses or severity over a period of time to give a final probability distribution.

The combination process merges the distribution curves of projected cyber loss events with that of the severity or loss curve. The two merged distribution curves would always be discrete in nature and therefore it is necessary to fit to the best curve. The convolution process is completed when the two curves are successfully merged to give the final probability loss distribution curve. Steps leading up to the process are shown in Figure 4:

[16] In the case of the Poisson distribution, this simple approach is supported by the fact that the Maximum Likelihood Estimate of the single Poisson parameter is equal to the mean frequency. The negative binomial distribution could provide additional flexibility in specifying the distribution shape, but this only becomes relevant for higher-frequency events, which are not being considered here

[17] All accompanying models are developed by BBA

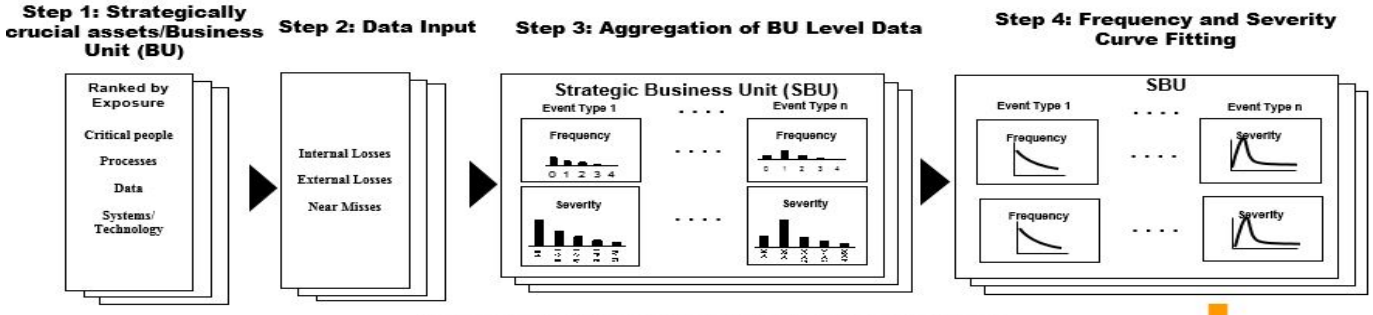
[18] The Poisson distribution assumes that events are independent, the probability of an event is constant through the sequences of intervals, and the probability of an event is proportional to the size of the interval.

[19] The Pareto probability density function (first kind) is sourced from Klugman et al., Loss Models: From Data to Decisions, 1998. This distribution is a special case of the transformed beta distribution, which has four parameters

[20] Generalized Pareto Distribution is also used by Fitch for scenario analysis purposes

[21] Convolution process is a mathematical way of combining two signals to form a third signal

Figure 4: Convolution



	External Fraud	Internal Fraud	Damage to Physical Assets	Execution Delivery and Process Management	Business Disruption and System Failures	Execution Delivery and Process Management	Clients, Products, and Business Processes	VaR ($)
Scenario 1: Phishing	X			X	X	X		
Scenario 2: Ransomware					X		X	
Scenario 3: Data breach/Hack	X	X			X	X	X	
.		X						
.			X		X	X	X	
.			X	X	X	X	X	
Scenario (n): Malware			X	X	X	X	X	

3.6. Step 6: Simulation

In practical terms, Maximum Likelihood estimation is an optimization procedure that searches for the set of parameters that will maximize the likelihood function. Intuitively, it is the set of parameters of the distribution that the data 'most likely came from'. There are several strong statistical properties that draw practitioners to this estimation procedure. In particular, for large samples, Maximum Likelihood parameter estimates are asymptotically normally distributed, asymptotically 'minimum variance' and asymptotically unbiased. These nice properties come at a price. Maximum Likelihood estimation requires non-linear optimization routines to search for the optimal set of parameters that maximize the specified likelihood function. This is not straightforward. Often, the nonlinearities in the likelihood function result in many 'local maximia', which can trick the analyst into believing they are global maxima. To overcome this problem, it is important to have advanced optimization routines to capture the true likelihood maximum.

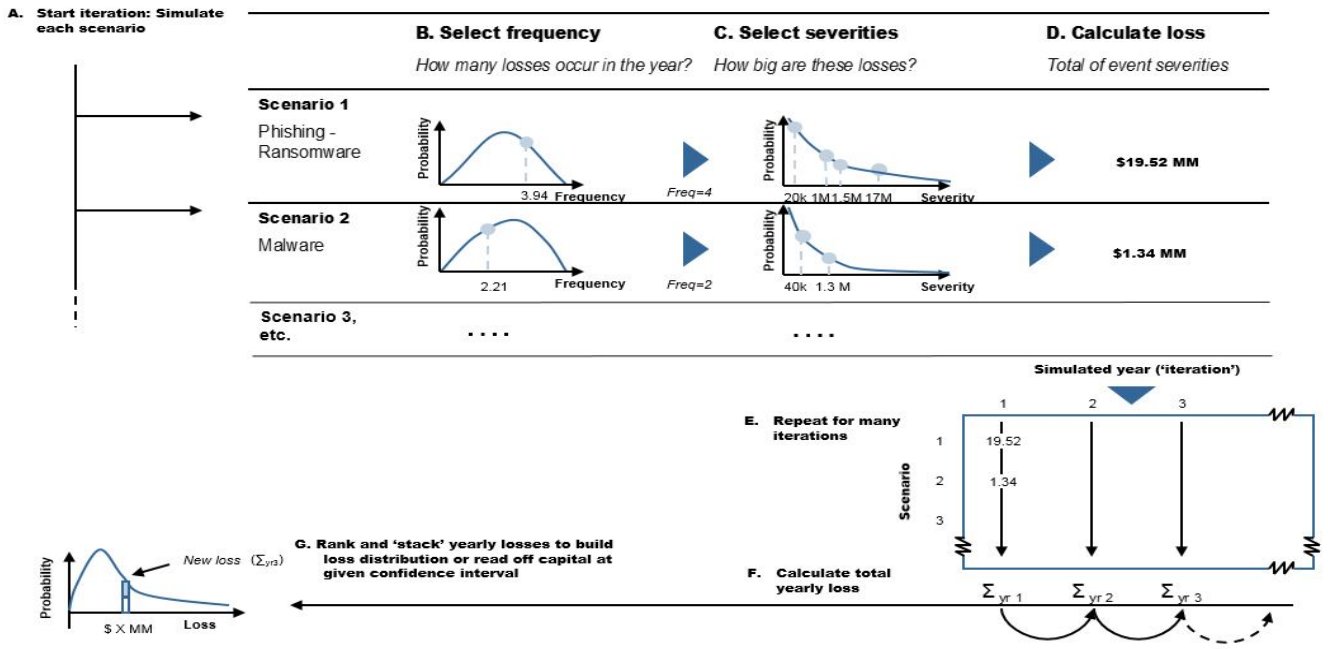
Monte Carlo simulation is utilized to solve the open form solution of the convolution process by performing statistical sampling experiments (Figure 5). This procedure requires a precise overall characterization of both distributions.

The total annual loss distribution is the distribution of total operational cyber risk losses that can occur over the next 12 months. A simplified Monte Carlo approach works as follows:

1. Develop accurate parameterization of the scenarios for each asset cohort type.
2. Determine frequency and severity for cyber loss events.
3. From the frequency distribution for the 'body' of e.g., Ransomware, draw a number of loss events.
4. From the severity distribution for the 'body', e.g., Ransomware, draw a number of losses.
5. Calculate the sum of "Ransomware" number of losses, yielding the total annual 'body' loss in the simulated year.
6. Repeat the above 3 steps for the 'tail' of "Ransomware" and the 'body' and 'tail' of other loss scenarios, yielding separate total annual 'body' and 'tail' losses for each of the cyber loss events.
7. Sum together the 'body' and 'tail' losses for each of the cyber losses, yielding a total annual loss per scenario.
8. Sum together the losses to produce a total annual loss, representing one data point in the total annual loss distribution.
9. Repeat steps a large number of times (n iterations) to simulate the full range of potential annual outcomes.
10. Repeat steps a number of times (m runs) to carry out multiple simulations.

The model assumes no correlation between either severities or frequencies. The lack of correlation is likely to be a good first-cut approximation of reality. In addition, scenario independence also makes the modelling much faster and simpler. For each iteration, the model selects each scenario in turn, determines whether that event occurs or not, and the severity of the event if it occurs. It then sums together the 'body' and 'tail' losses for each of the scenarios, yielding a total annual loss per scenario. The total loss for each year is then stored and used to build up a distribution of potential losses.

Figure 5: Procedure for a single run of the Monte Carlo simulation process



Scenario analysis provides the best way to understand the relevance of external data to specific circumstances and make sensible adjustments.

3.7. Step 7: Loss adjustment using control scorecard

Once cyber loss estimates are determined for each cohort across business units, KRIs can be drawn together for each business unit. The KRIs are then evaluated for controls against the potential losses. Various approaches can be developed to allocate capital based on the effectiveness of controls at each business unit. Some of the questions that need to be answered are:

- What is the purpose of the scorecards?
- Are scorecards linked to performance measurement?
- How far should capital allocation be driven down?

The capital adjustment equation is:

$$C_{adj,i} = (1 - A_i) * C_{LDA,i}$$

$C_{adj,i}$ is adjusted capital (pre group-level reconciliation) for business unit i.

$C_{LDA,i}$ is capital implied by Loss Distribution Approach (LDA) for business unit *i.*

A_i *is* capital adjustment factor, determined as follows:

$$A_i = (w_{\propto_i} * \propto_i) + (w_{\propto'_i} * \propto'_i)$$

$w_{\propto_i}$ is Weight applied to "level" adjustment factor[22] for business unit *i.*

$\propto_i$ is Level adjustment factor for business unit *i* (captures differences in absolute levels of residual risk across business units).

$w_{\propto'_i}$ Weight applied to change adjustment factor for Business Unit *i.*

$\propto'_i$ Change adjustment factor for Business Unit *i* (captures differences in relative changes in risk profile across business units).

[22] Expert judgement adjustment factors can be designed based on incidents report card. For example, risk culture, training of the staff, historic cyber hygiene, etc.

4. BUSINESS CYBER RISK QUANTIFICATION

Mostly, the knock-on effect of cyber events, such as loss of reputation, are not captured by cyber operational risk modelling. Some examples of the secondary impact of the cyber-attacks are:

- Negative media coverage
- Loss of credibility
- Reputational loss
- Loss of customer-base
- Credit rating downgrade
- Significant drop in share price
- Fines

Despite seemingly having the resources to contend with cybercrimes, large, highly valued, and visible firms — such as Fortune 500 companies — are attacked most often. Companies that use customers' personal data to conduct daily business, such as those in the financial and retail sectors, are also more frequent targets, regardless of size. But financially constrained firms are rarely targeted[23].

Successful cyber-attacks can also result in heavy fines. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are two examples. Under GDPR, failure to safeguard data and privacy can lead to fines of up to €20 million or 4% of the annual worldwide revenue of the preceding financial year, whichever is greater[24]. Under CCPA violators are fined $7,500 per record stolen[25].

Figure 6 shows stages of deterioration in earnings as a result of a loss event.

Properly designed, an earnings volatility model provides a better understanding of the drivers of volatility and also offers planning considerations. This enables consideration of both earnings growth and earnings volatility in seeking to maximize the economic value of an organization.

Figure 6: Stages of earnings shortfall

4.1. Modelling business risk

Business risk capital is the amount of capital required to hold against unexpected operating losses. Operating losses are defined here as those not attributable to position-taking (which are covered by market risk capital) or counterparty default (covered by credit risk capital). Typically, unexpected operating losses arise from a fall in volumes. The calculation of business risk capital charge is based on the following assumptions:

- There is a known fixed cost base (non-volume dependent) which does not contribute to uncertainty. It is independent of volumes. Fixed costs should capture all costs a unit will have to pay throughout the year, excepting only the truly marginal costs associated with transactions. Fixed costs therefore include:
    - Overheads
    - Premises or rent
    - Salaries and other personnel costs for permanent staff
    - Leased equipment
    - Contracted services
    - Depreciation of assets
- Volume-dependent costs (VDC) increase with volumes and are zero when volumes are zero. These are costs which could be erased over a one year time horizon if volumes

[23] [Kamiya 2018]
[24] The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA) which came into effect on May 25, 2018. Source: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[25] [Government of California, 2019]

CCPA requires the reporting of not only the theft of Social Security numbers, driver's license numbers, banking information, passwords, medical and health insurance information, but also if passport and government ID numbers, along with biometric data, such as fingerprints, and iris and facial recognition scans, have been stolen. Individuals can bring a lawsuit if there's been a data breach and a company isn't using reasonable security measures to protect information being gathered. That's on top of the $7,500 per record fine that can be assessed by the Attorney General under CCPA

were to fall. Operating Revenue (OR) is revenue derived from margins, spreads and commissions. Variable Margin (VM) is log-normally distributed and defined as:

$$VM = OR - VDC$$

- The lower bound of variable margin is zero, since volume dependent costs are always less than Operating Revenue in a stable business, and neither can be negative.

In a mature business, variable margin is log-normally distributed with mean μ_{VM} and standard deviation σ_{VM}. Worst case variable margin at the appropriate confidence interval is calculated from the normal distribution of LnVM[26] with mean μ_{LnVM} and standard deviation σ_{LnVM}.

Business risk capital is thus defined in terms of a multiple, m, of the volatility of variable margin. The value of the multiple is determined from the desired solvency standard.

$$WorstcaseVM_{Desired\ Solvency\ Standard} = e^{(\mu_{LNVM} - m.\sigma_{LNVM})}$$

The difference between mean VM and worst case VM is the amount of business risk capital:

$$Businessrisk\ capital = \mu_{VM} - WorstCaseVM_{Desired\ Solvency\ Standard}$$

In a growing business the approach needs to be modified, as the mean variable margin over previous years is likely to be less than that expected or forecast in the future. Therefore, current revenue and expense data are used to calculate the 'mean' variable margin. In addition, if the volatility of variable margin is being proxied by, say, net volume inflows these should be normalized against total volume, to provide a constant measure of volatility over time.[27]

5. SYSTEMIC CYBER RISK QUANTIFICATION

Cyber-attack risk has been identified by the World Economic Forum as a main concern among market participants and was ranked first as a threat to systemic stability. In a paper published last year[28], the International Monetary Fund also described cyber risk as a key threat to financial stability. Rising cross-border cyber-attacks make cyber risk increasingly international.

The Office of Financial Research of the US Department of Treasury[29] also published a survey of studies of empirical measures aimed at identifying systemic risks (31 quantitative measures overall). While the review does not point out a universal definition and measure of systemic risk, it identifies key common properties of different approaches and concludes that more than one risk measure will be necessary to capture the complexities of cyber-attacks. Among these, the common properties are:

- Correlated exposure, e.g., business interruption losses can far exceed direct damage, reputational risk;
- Negative externalities, e.g., an attack or event that impacts the financial system may come from a source exogenous to the system; as an example: an infiltration coming from critical service providers in computing, telecommunications, or energy, and;
- Transmission mechanism with a threat multiplier, e.g., WannaCry ransomware attack as described in figure 7.

Figure 7: WannaCry Chronology of Events

US intelligence officials testified in January 2017 that as of late 2016, more than 30 governments were actively developing offensive cyber-attack capabilities.[30]

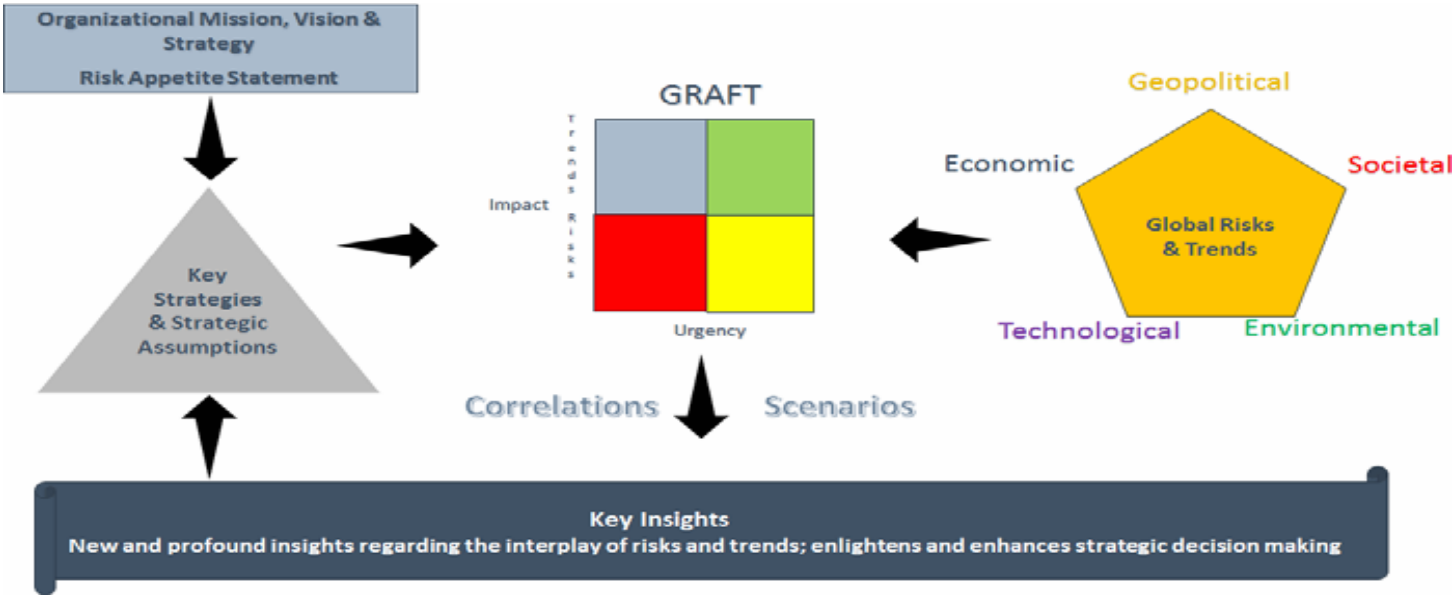
The WannaCry global ransomware attack which impacted legacy technology within the National Health Service (NHS) was reportedly rooted in a compromise of US government intelligence tools, monetized by Russian-linked criminals and weaponized by the North Korean state (DPRK)[31].

[26] The natural logarithm of a number is its logarithm to the base of the mathematical constant e
[27] Monte Carlo scenarios will be covered in follow on research
[28] Bouveret 2018]
[29] [Cebula 2014]
[30] [Clapper, US Senate, 2017]
[31] [Graham, 2017]

5.1. Introducing Global Risks and Trends Framework (GRAFT)

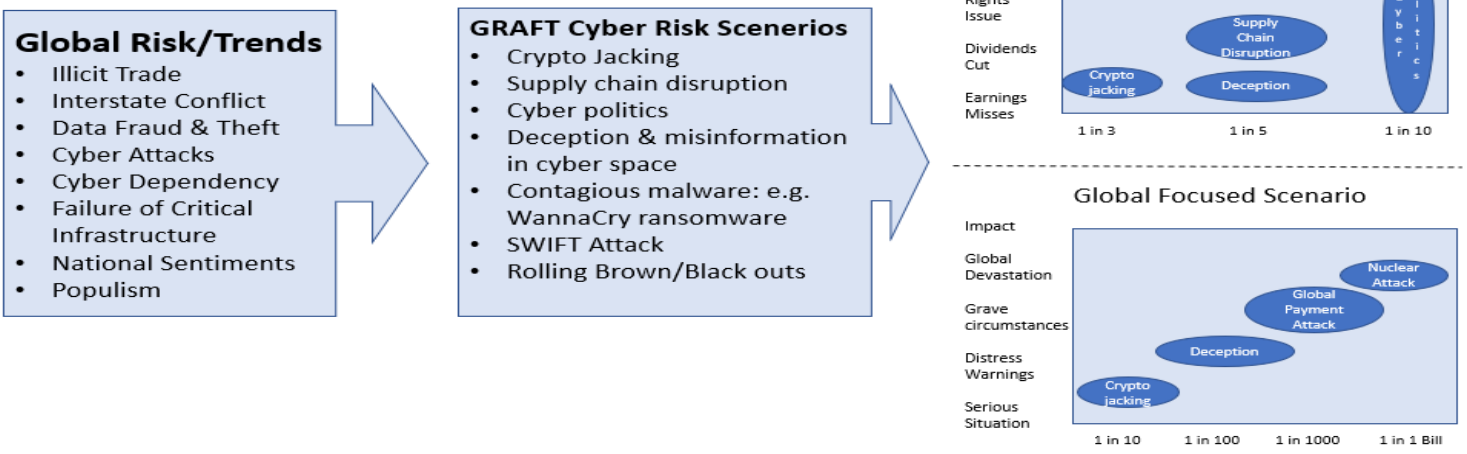
So far, the focus of this paper has been on the idiosyncratic features of cyber risk, however, it is the systemic impact of cyber risk that is seemingly getting more attention, both from the regulators and also from the cyber criminals. GRAFT[32] scenarios helps us develop a better understanding of the systemic risks' impacts and stresses on the business risk by testing assumptions and strategy, as shown in the graphic below:

Figure 8: Overview of GRAFT Framework



The GRAFT framework links the Global Risks and Trends to the organizations' strategy, through identifying the strategic assumptions that the strategy is based upon. The risks and trends are prioritized based upon their impact (severity & probability) and their urgency. They are assessed upon their correlation and inter-relationship, to provide directionality to scenario analysis and stress testing. These scenarios are parameterized to assess the impact on growth, income and capital. Typically, experts conduct workshops to develop consensus scenarios and also help with their parameterization. An example of how the GRAFT framework assists with scenario finalization is shown in Figure 9.

Figure 9: Scenario design with GRAFT



[32] [Tullo 2017] The Global Risks and Trends Framework
GRAFT is a new approach designed to help organizations identify, assess and respond to global risks and trends in order to avoid pitfalls that could threaten an organizations long-term survival or conversely to leverage for the benefit of the organization

5.2. Calculating Systemic Cyber Risk

Calculating the impact of the global risks and trends on the probability, severity, and timing of cyber-attacks can make use of either regression analysis (covered in this paper and model) or use of the artificial neural networks (ANNs) statistical learning model. ANNs are statistical learning models, inspired by biological neural networks (such as the brain), that are also used in machine learning.

To investigate the impact of GRAFT scenarios on earnings, we start with a long list of factors. For example, breakdown of governance could imply shutting-down the airspace or national stock markets for an extended period. Using the latter scenario, this implies an impact on the liquidity of financial institutions.

Business risk and earnings at risk (EaR) underpin business risk as maximum frequency of earnings shortfalls of a given severity. Once top-down GRAFT scenarios are defined, we can develop explanatory variables from the scenarios to forecast earnings volatility.

The earnings volatility rate can be thought of as a function of the values of the systemic risk factors triggered by GRAFT scenarios ($\overrightarrow{x_1}$, $\overrightarrow{x_2}$ and $\overrightarrow{x_3}$).[33] These factors could be stock market crash, inflation, etc.

$$\widehat{EaR} \sim f(\overrightarrow{x_1}, \overrightarrow{x_2}, \overrightarrow{x_3}).$$

Agreeing on the risk drivers or scenarios parameters is quite important. An objective approach entails running regressions to establish how risk drivers impact the dependent variable (earnings volatility). The selection of risk drivers for the volatility model should be considered as an iterative exercise with pre-dominant role of an expert opinion in selecting risk drivers.[34] Typically, an R-squared (R^2) statistic of > 60% needs to be targeted.

$$\widehat{EaR}_{\propto} = NI_{t-1}(1 - \exp(\mu_{L/P} - \sigma_{L/P} z_{\propto}))$$

NI_{t-1} Last period's net income

$\mu_{L/P}$ is the mean of earnings

$\sigma_{L/P}$ is the standard deviation of earnings

$z_{\propto}$ is the confidence level

Once the systemic risk parameters are finalized, experts can then forecast medium term values for both the base and stressed GRAFT cases.

Some important considerations include:

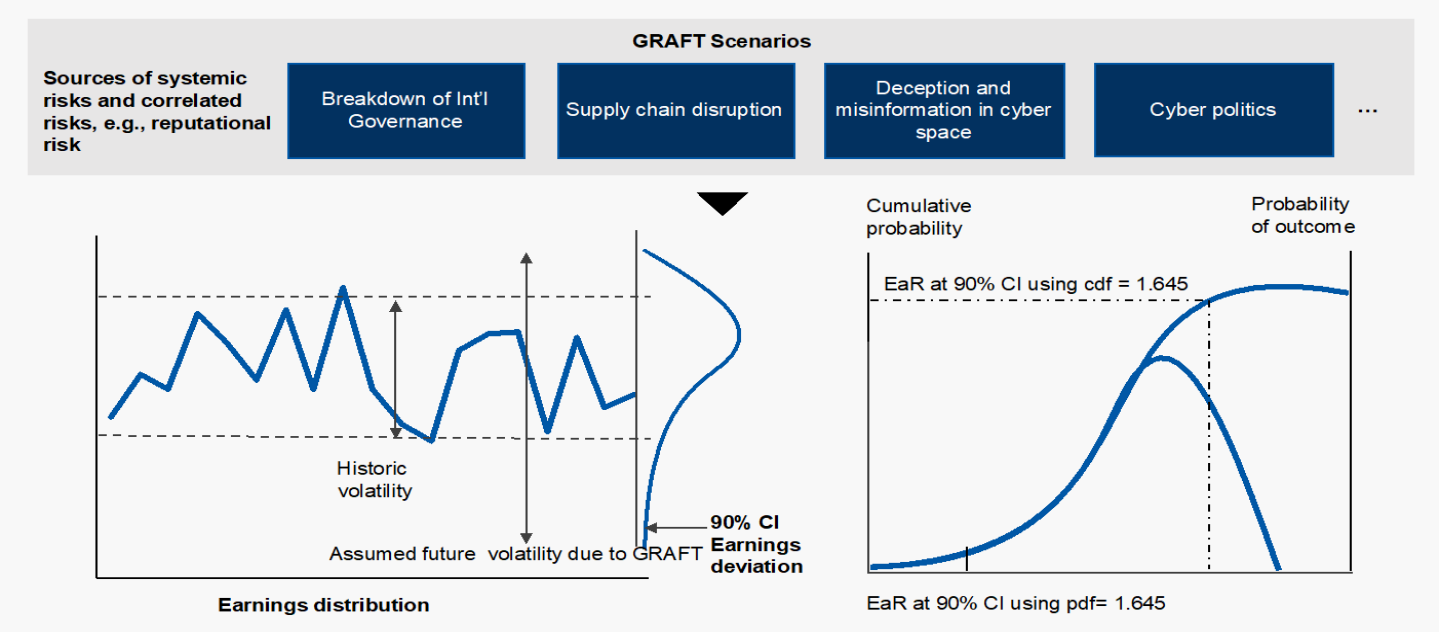
- Factors from the extended list that did not pass a set of ex-ante defined criteria, such as expert opinion to be removed from consideration;
- Quantitative analysis to be carried out only on those factors which were previously demonstrated to be highly predictive of losses;
- Intuitive sign of relationship;
- Limited factor complexity.

The EaR metric is broadly based on economic capital methodology, which uses past volatility of returns per business unit, scaled to a 90% confidence interval using the t-distribution (the degrees of freedom can be set equal to the number of quarters of available earnings figures less one). Once per economic cycle frequency has, in many ways, become the industry standard for measuring cyber risk. Figure 10 illustrates 90% EaR for a normally distributed P/L. In this case, EaR is given by the point on the x-axis that cuts off the top 10% of probability distribution function (pdf) mass from the bottom 90% of pdf mass.

[33] $\overrightarrow{x_1}$, $\overrightarrow{x_2}$and $\overrightarrow{x_3}$ are sample means of systemic volatility factors

[34] A more objective approach is to use Single Factor Analysis

Figure 10: Normally Distributed Earnings Data



The figure above uses a Z score prediction model for each normalized regression variable (factors) to predict the earnings volatility (2 – 3 years) for both the base case and stressed GRAFT scenario(s). We create a new standardized version of each variable by transforming predictors to a standard Z scale. This allows a comparison between the dependent and independent variables. Using the set of equations below, we can forecast earnings volatility:

$$\hat{Z}_{Y_{BASE_t}} = (\beta_1)\left(Z_{x_{1_{BASE_t}}}\right) + (\beta_2)\left(Z_{x_{2_{BASE_t}}}\right) + \cdots (\beta_n)\left(Z_{x_{n_{BASE_t}}}\right)$$

$$\hat{Z}_{Y_{GRAFT_t}} = (\beta_1)\left(Z_{x_{1_{GRAFT_t}}}\right) + (\beta_2)\left(Z_{x_{2_{GRAFT_t}}}\right) + \cdots (\beta_n)\left(Z_{x_{n_{GRAFT_t}}}\right)$$

$$\sigma_t = \frac{(\hat{Z}_{Y_{BASE_t}} - \hat{Z}_{Y_{GRAFT_t}})}{n-1}$$

Z score is determined as follows:

$$Z_{x_{i_{GRAFT_t}}} = \frac{(X_{i_{GRAFT_t}} - M_{x_{i_{ACTUAL}}})}{SD_{x_{i_{ACTUAL}}}}$$

Forecasted Earnings at risk is:

$$\widehat{EaR}_{t+1_\propto} = NI_t(1 - \exp(\mu_t - \sigma_t z_\propto))$$

$\hat{Z}_{Y_{BASE_t}}$ is the base case earnings forecast at time t $\hat{Z}_{Y_{GRAFT_t}}$ is GRAFT earnings forecast at time t.

$\beta_1 \ldots . \beta_n$ are coefficients of independent variables (can be thought of as weights vector).

$Z_{x_{i_{BASE_t}}}$ is standardized predictor for variable x_i under base case.

$Z_{x_{i_{GRAFT_t}}}$ is standardized predictor for variable x_i for under GRAFT scenario.

$M_{x_{i_{ACTUAL}}}$ is the mean of i^{th} predictor variable.

$SD_{x_{i_{ACTUAL}}}$ is the standard deviation of i^{th} predictor variable.

NI_t Current period's net income.

$\widehat{EaR}_{t+1_\propto}$ Earnings at risk forecast estimate.

$\propto$ is confidence leve.l

Given a large-scale cyber-attack, we can analyze the risk propagation throughout the system using GRAFT and quantify the knock-on impacts of the event using the DAIR modelling framework.

6. INSURABILITY OF CYBER RISK

Modelling insurance involves the consideration of detailed event descriptions on a case-by-case basis. However, the capital-reducing effect of insurance is still difficult to quantify as insurance typically has the greatest impact on medium-sized losses, which contribute little to capital requirements. In addition, due to per-claim limits, insurance tends to have a small impact on extreme losses, which drive capital.

Nonetheless, disregarding insurance outrightly may be undesirable as it does influence protection against earnings deviation. It is important both for modeling and for business clarity to identify explicit cyber insurance coverage and to identify the areas of "silent" or "non-affirmative" cyber insurance. Silent cyber is an exposure on an insurance line of business derived from some sort of computer system, software, virus or malicious code. There is coverage ambiguity. Coverage is neither explicitly included or excluded.[35] The scope and definition of insurance would vary due to disparate insurance coverages by providers and are therefore hard to standardize.

7. CONCLUSION

The management of cyber risk is complex and evolving, and financial institutions around the globe are at different starting points. To integrate cyber risk with broader risk management, all parties must speak the same language. Consolidation of cyber into a single organization-wide taxonomy reduces the number of risk types. This helps avoid pitfalls when used to assign responsibilities to second line functions.

By quantifying cyber risk, financial institutions can improve control frameworks and prevent attacks. The size and complexity of an organization will influence its approach. With DAIR's three different approaches to choose from, any one of them can be used as a pilot to enable better risk management and lower the cost of compliance.

DAIR can also be used for the roll-out of the risk appetite limits by answering the following questions:

- What is our aggregate cyber risk exposure?
- What is our operational risk capital charge and how much of that can be delineated to cyber risk?
- How can we refine and improve the threshold limits for the key risk indicators and make our controls more effective?
- What level of exposure are we willing to accept, insure and charge to our capital?
- How much should we invest in cyber risk mitigation and what is our return on investment?
- How can we assign the contribution of cyber/security risk costs in risk-based pricing frameworks?

Despite the lack of model data - often due to a high proportion of unreported attacks - the impact-driven methodologies presented in this paper can easily be implemented using internal and external benchmarks. Finally, the prize of an integrated DAIR framework is not only regulatory compliance but also business benefits in the form of lower risk costs and attribution of business cyber risk in product pricing.

[35] This paper views cyber insurance as the most relevant cyber cost. If data theft is the result of a cyber breach then it is covered under the insurance consideration. However, general fraud insurance is outside the scope of the methodology.

Appendix 1: Survey of existing risk assessment approaches

Office of the Superintendent of Financial Institutions (OFSI)

While OSFI generally does not require a specific cyber strategy, federally regulated financial institutions (FRFIs) in Canada are expected to maintain adequate capability in this area. OSFI encourages FRFIs to undertake cyber-security self-assessment. OSFI's cyber-security self-assessment is organized in the following six areas of focus:

(1) Organization and resources
(2) Cyber risk and control assessment
(3) Situational awareness
(4) Threat and vulnerability risk management
(5) Cyber security incident management
(6) Cyber security governance

Self-assessment outcomes are also rated on a 1 to 4 scale based on the degree of maturity.

Canadian Cyber Threat Exchange (CCTX)

CCTX is Canada's only cyber threat collaboration forum and source of cyber threat intelligence. The CCTX was created to build a secure Canada where all organizations, both private and public, collaborate to reduce cyber security risks. CCTX does this in two ways:

(1) First, through the CCTX Data Exchange which gathers and shares cyber threat information across business sectors and from other Canadian and international cyber threat sharing hubs;
(2) Second, through the CCTX Collaboration Centre which is a unique forum for cyber professionals to solve problems by exchanging best practices, techniques and insights.

Federal Financial Institutions Examination Council (FFIEC)

In the United States, the (FFIEC) released the cybersecurity assessment tool (Assessment) to help institutions of all sizes identify their risks, assess their cybersecurity preparedness, and inform their risk management strategies.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

Using the information outlined in the FFIEC's Assessment, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) developed the automated cybersecurity assessment Tool to provide all members of the financial services industry with an outline of the guidance and a means to collect and score their responses to the assessment questions.

FSSCC is one of sixteen sector-specific industry collaborators formed under a 2003 executive order that established a framework for public-private partnership to address security and resilience of the nation's critical infrastructures. The FSSCC is focused on addressing operational and strategic risks.

The FSSCC coordinates the development of critical infrastructure strategies and initiatives with its financial services members, trade associations, and other industry sectors.

Federal Information Security Management Act

FISMA is a United States federal law enacted in 2002. The compliance framework under FISMA has brought attention within the federal government to cybersecurity and explicitly emphasizes a "risk-based policy for cost-effective security."

The National Institute of Standard and Technology (NIST)'s cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

FAIR framework

According to The Open Group's Technical Standard a basic risk assessment using FAIR's taxonomy can be undertaken as follows:

Stage 1: Identify scenario components:

- Identify the asset at risk.
- Identify the threat community under consideration.

Stage 2: Evaluate loss event frequency (LEF):

- Estimate the probable threat event frequency (TEF).
- Estimate the threat capability (TCap).
- Estimate control strength (CS).
- Derive vulnerability (Vuln).
- Derive loss event frequency (LEF).

Stage 3: Evaluate probable loss magnitude (PLM):

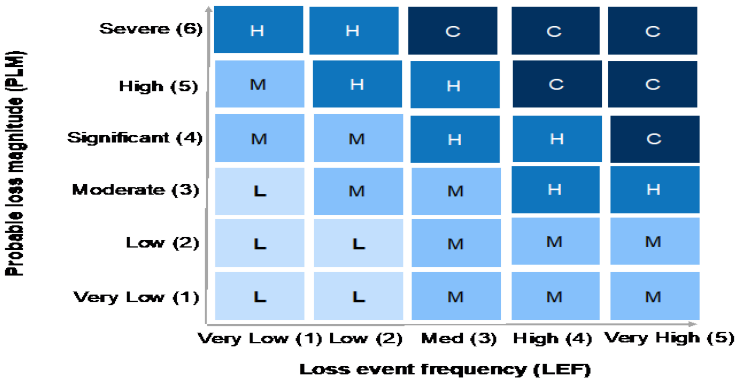
- Estimate worst-case loss.
- Estimate probable loss magnitude (PLM).

Stage 4: Derive and articulate risk:

- Derive and articulate risk.

When applied to cyber risk management this means that organizations begin with a comprehensive survey to identify assets at risk and threat communities. Stages 2 and 3 are based on subjective assessment due to limited historic data. The assessment concludes (Stage 4) by articulating risk based on the following matrix:

Risk matrix[36]



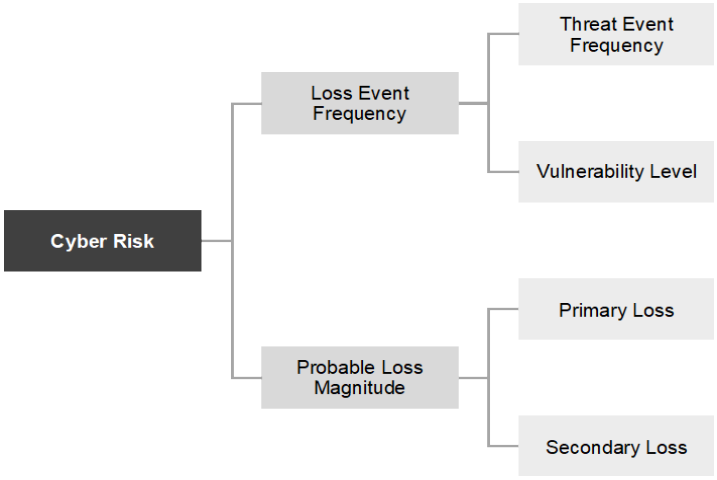
Appendix 2: FAIR taxonomy component definitions[37]

Risk

Risk is the probable frequency and probable magnitude of future loss. With this as a starting point, the first two obvious components of risk are loss frequency and loss magnitude. In The Open Group's Technical Standard, these are referred to, respectively, as loss event frequency (LEF) and probable loss magnitude (PLM).

Loss event frequency (LEF)

LEF is the occurrence, within a given timeframe, that a threat agent will inflict harm upon an asset. In order for a loss event to occur, a threat agent has to act upon an asset, such that loss results.



Threat event frequency (TEF)

TEF is the occurrence, within a given timeframe, that a threat agent will act against an asset. Threat agents may act against assets, but be unsuccessful in affecting the asset. A common example would be the hacker who unsuccessfully attacks a web server. Such an attack would be considered a threat event, but not a loss event.

Vulnerability

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force.

Vulnerability is always relative to the type of force and vector involved. For example, a computer anti-virus product doesn't provide much in the way of protection from the internal employee seeking to perpetrate fraud. The key, then, is to evaluate vulnerability in the context of specific threat types and control types.

Probable loss magnitude (PLM)

PLM is the likely outcome of a threat event.

An asset's loss potential stems from the value it represents and/or the liability it introduces to an organization. For example, customer information provides value through its role in generating revenue for a commercial organization. That same information can also introduce liability to the organization if a legal duty exists to protect it, or if customers

[36] Technical Standard [2009], pp. 32

[37] Technical Standard [2009], pp. 11

have an expectation that the information about them will be appropriately protected.

Six forms of loss are defined within the Technical Standard, as follows:

- Productivity – the reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services, etc.).
- Response – expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.).
- Replacement – the intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop, etc.).
- Fines and judgments (F/J) – legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.
- Competitive advantage (CA) – losses associated with diminished competitive advantage. Within this framework, CA loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Within the commercial world, examples would include trade secrets, merger and acquisition plans, etc. Outside the commercial world, examples would include military secrets, secret alliances, etc.
- Reputation – losses associated with an external perception that an organization's leadership is incompetent, criminal, or unethical.

Primary loss factors (PLF)

There are two asset loss factors: asset loss factors and threat loss factors. Asset Loss Factors are: value/liability and volume. Threat Loss Factors include: action, competence, and whether the threat agent is internal or external to the organization.

Secondary loss factors

Secondary loss factors are those organizational and external characteristics of the environment that influence the nature and degree of loss.

References

[Biener, 2018]

Biener, Christian; Eling, Martin & Wirfs, Jan Hendrik. *Insurability of Cyber Risk: An Empirical Analysis* University of St. Gallen, Institute of Insurance Economics, WP on Risk Management and Insurance No. 151

https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

[Kamiya, 2018]

Kamiya, Shinichi; Kang, Jun-koo; Kim, Jungmin; Milidonis, Andreas; Stulz & René M. *What is the impact of successful cyberattacks on target firms?* Dice Center WP 2018-4, Fisher College of Business WP 2018-03-04

http://www.ssrn.com/abstract=3135514

[Jones, 2009]

Jones, Jack A. *An Introduction to Factor Analysis of Information Risk (FAIR)*

The Open Group Technical Standard to Risk Taxonomy Number C081

http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf

[The Open Group, 2009]

The Open Group. *Technical Standard to Risk Taxonomy*. Number C081

https://www.opengroup.org

[Cebula, 2014]

Cebula, James J.; Popeck, Mary E.; Young, Lisa R., *A Taxonomy of Operational Cyber Security Risks Version 2* Technical Note CMU/SEI-2014-TN-006

http://www.sei.cmu.edu

[BCBS 2006]

International convergence of capital measurement and capital standards: A revised framework (comprehensive version). Basel, Switzerland: Basel Committee on Banking Supervision, Bank for International Settlements

https://www.bis.org/publ/bcbs128.htm

[Agrafiotis 2018]

Agrafiotis, Ioannis; Nurse, Jason R. C.; Goldsmith, Michael; Creese, Sadie; and Upton, David. *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate*. Journal of Cybersecurity, 1–15.

https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288

[Bouveret 2018]

Bouveret, Antoine. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.* IMF Working Paper.

https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

[Fishburn 1977]

Fishburn, Peter C. *Mean-Risk Analysis with Risk Associated with Below-Target Returns.* The American Economic Review.

https://www.jstor.org/stable/pdf/1807225.pdf?seq=1#page_scan_tab_contents

[Jankensgård 2008]

Jankensgård, Håkan. *Cash-Flow-at-Risk and Debt Capacity.* Lund Institute of Economic Research.

https://portal.research.lu.se/portal/en/publications/cashflowatrisk-and-debt-capacity(3375d4c9-f344-4e3c-9107-eefead5d6943).html

[Tullo 2017]

Tullo, Lois. A Global Risks and Trends Framework: Overview

https://globalriskinstitute.org/publications/global-risks-trends-framework-graft-overview