RISCS

CYBER RISK QUANTIFICATION RESEARCH PROJECT

Identification and Feasibility Assessment of Options for a Standard Model for Costing Cyber Security Incidents

PROJECT TEAM:
Alpesh Bhudia, Anna Cartwright, Edward Cartwright, Frank Cremer, Tom Meurs, Phillip Samson, Jacob Seifert, Darren Shannon, Barry Sheehan.

VERSION 1.0
26/03/24

OXFORD BROOKES UNIVERSITY
DE MONTFORT UNIVERSITY LEICESTER
UNIVERSITY OF LEICESTER
UNIVERSITY OF LIMERICK OLLSCOIL LUIMNIGH

RISCS

Table of Contents

Executive Summary

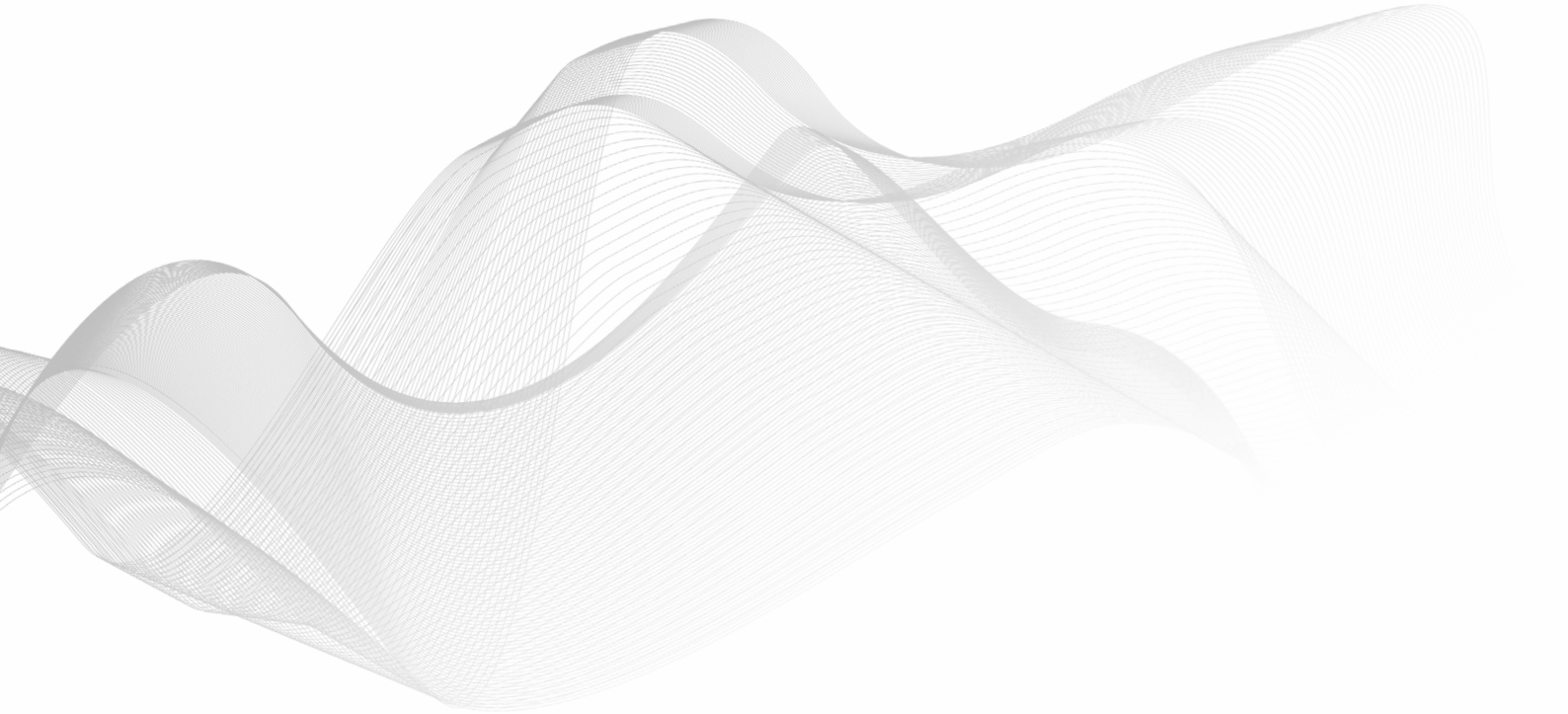
To inform cyber security policy, risk management and quantification, it is vital to have appropriate methods to measure the cost of a cyber incident. However, there is currently no internationally agreed-upon way to model the cost of a cybersecurity incident. In this report, we explore options for identifying a standard model for costing cyber incidents. In doing so, we overview existing approaches for assessing the cost of incidents and consider the pros and cons of quantifying incidents before outlining recommendations on the use of standardised approaches for costing cyber security incidents.

OUR KEY FINDINGS

1. There exist evidence-based taxonomies of cyber harms that provide a good framework for estimating the cost of a cyber incident. Such taxonomies cover a wide range of costs, including psychological and societal harms.

2. There are well-established methods to estimate the costs of a cyber incident, using a Value at Risk approach (VaR). It is not clear, however, to what extent such methods currently capture all of the harms from an incident or take into account opportunity costs and attributable costs.

3. Building on existing approaches, particularly in terms of costing intangible loss, we believe it is feasible to develop a standard model of costing a cyber incident that would be applicable to most organisations and types of cyber incidents.



Our key recommendations for a standard model of costing a cyber incident can be summarised:

1. A standard model needs to take into account the desired output of the user. For instance, the needs of a business or insurer in costing an incident may be very different to those of a government department or regulator. The scope of the costing exercise should be clear, e.g., whether social or spillover costs are included.

2. The model needs to take account of intangible as well as tangible costs, e.g., psychological costs to staff impacted by the incident and loss of reputation to the firm. Various economic approaches exist to quantify intangibles, e.g., using loss of productivity and/or loss of staff time due to sickness as measures of psychological impact.

3. The model should be clear and transparent in the assumptions used to cost the incident, e.g., discount rate, calculation of downtime and calculation of staff time, as well as methods, e.g., accounting versus economic cost. The model should be flexible to allow for different underlying assumptions, e.g., estimating the cost of the incident for different values of the discount rate.

4. The model needs to recognise the long-run costs of a cyber incident. The long-run costs of an incident (e.g., reputation loss) are difficult to quantify in the short run. The model needs, therefore, to allow for updates over time as new information becomes available.

5. The model should provide clear guidance on how to calculate the cost and, crucially, outline the data required to input into the calculation exercise. The organisation should perform mock exercises to verify that it would be in a position to capture the data required to calculate the cost of an attack. An evaluation of costs needs input from across the organisation, including IT, finance, HR, and senior management.

6. A cyber incident can have 'benefits' for an organisation, particularly in terms of 'learning from experience'. However, these benefits should typically not be included in the costing of the cyber incident. Instead, the notion of opportunity cost should be invoked with a focus on attributable costs and whether the organisation could have 'learnt from experience' without the attack. In most instances, there are resources and information that could have enabled the organisation to improve its cyber security and would have been less costly than a cyber-attack.

7. The model should reflect the resources and capabilities of the organisation to perform the exercise. For example, a small business will have less capability to perform a complex costing exercise. Crucially, the model should not seek simplification by narrowing scope because intangible losses (e.g., psychological stress) are particularly relevant for small organisations. Instead, the model needs to provide sufficient guidance and support to be simple to implement.

List of Abbreviations

AHP	Analytical Hierarchical Process
AIR	Applied Insurance Research
CVaR	Cyber Value at Risk
DDoS	Distributed Denial-of-Service
FAIR	Factor Analysis of Information Risk
MCDM	Multi-Criteria Decision Making
NIST	National Institute of Standards and Technology
RCVaR	Real Cyber Value at Risk
RMS	Risk Management Solutions
VaR	Value at Risk
VERIS	Vocabulary for Event Recording and Incident Sharing

Introduction

Cyber attacks, such as ransomware, can have a massive impact on organisations and society. As a case in point, consider the ransomware attack on Hackney Council in October 2020, which impacted a wide range of public services for many months (Pattnaik 2023). To inform cyber security policy, risk management, and quantification, it is vital to have appropriate methods to measure the cost of such incidents (Anderson et al. 2013). It is, however, a highly complex task to estimate the costs of an attack. While the costs of employing consultants or investing in new assets may be readily quantifiable, the psychological costs to staff, loss in productivity, and the costs incurred from delayed access to services are much harder to quantify. A figure of £12 million was widely used by the media as the cost of the attack on Hackney Council, based on the Council's accounts for 2021-2022, but it is not transparent how this number was attained or how accurate it is.

In this report, we explore options for identifying a standard model for costing cyber incidents. Ideally, this standard model would provide a transparent method for organisations to cost cyber incidents and provide an accurate estimate of cost to inform policy. We first briefly overview the wide range of harms that can result from a cyber incident and discuss the importance of measuring opportunity cost. Next, we overview existing approaches for assessing the cost of incidents before considering the pros and cons of quantifying incidents. We finish by outlining a series of recommendations on the use of standardised approaches for costing cyber security incidents.

Categorising the Costs (and Benefits) of a Cyber Incident

In this section we will briefly overview the types of costs that can arise in a cyber incident and how the costs associated with an incident can be evaluated. Agrafiotis et al. (2018) provide a taxonomy of cyber harms. We take the approach in this report that an estimated financial cost can, in principle, be calculated for any harm that results from a cyber incident. In other words, harms resulting from an incident that are not initially financial in nature, such as psychological harm suffered by employees, can ultimately be translated into financial costs for the firm. Agrafiotis et al. (2018) distinguish the following five harm types (see also MacColl et al. 2024):

- **Physical or Digital Harm:** Costs incurred from e.g. damage, destruction, theft, modification, corruption of assets. For instance, systems or data encrypted, data exfiltrated, IT infrastructure not functioning, and backups being corrupted or destroyed.
- **Economic Harm:** Costs incurred from disruption of operations, regulatory fines, investigation and PR costs. It also includes any financial consequences in terms of e.g. customer loyalty, reduced investment, loss of employment, loss of intellectual property, and increase in insurance premiums.
- **Psychological and Physical Harm:** Psychological costs incurred from, e.g., panic, anxiety, depression, guilt, anger, and negative changes in perception. Physical costs incurred from exhaustion, sleep deprivation, burnout and serious illness.
- **Reputational Harm:** Costs incurred from, e.g., damaged public perception, reduced corporate goodwill, negative impact on relationships with clients, suppliers, and regulators, and reduced business opportunities. It also includes loss of staff and difficulty in recruiting new staff.
- **Social and Societal Harm:** Costs incurred from services in society not functioning as expected as negative changes in public perception. Also costs from strained relationships and family life.

As this taxonomy makes clear, there are many and varied ways in which a cyber incident can impact the organisation, its employees and society. A recent report by RUSI (MacColl et al. 2024) further distinguished between those directly and indirectly impacted by an incident:

- **First Order Harms:** Those directly incurred by the organisation (and its employees).
- **Second Order Harms:** Those indirectly impacted, such as clients and suppliers.
- **Third Order Harms:** capture the wider impact on society and the economy.

Another important factor to consider is time and a distinction between short, medium and long-run costs. In particular, Agrafiotis et al. (2018) highlight how a cyber incident will typically follow a sequence of events where costs are incurred. For instance, data exfiltration may lead to a ransom payment and/or a leak of data. The leak of data may subsequently lead to loss of reputation and loss of clients, which then has impacts on investment and profit. Decisions made at the start of a cyber incident will, therefore, impact the costs incurred as a result of the incident (Cartwright et al. 2023).

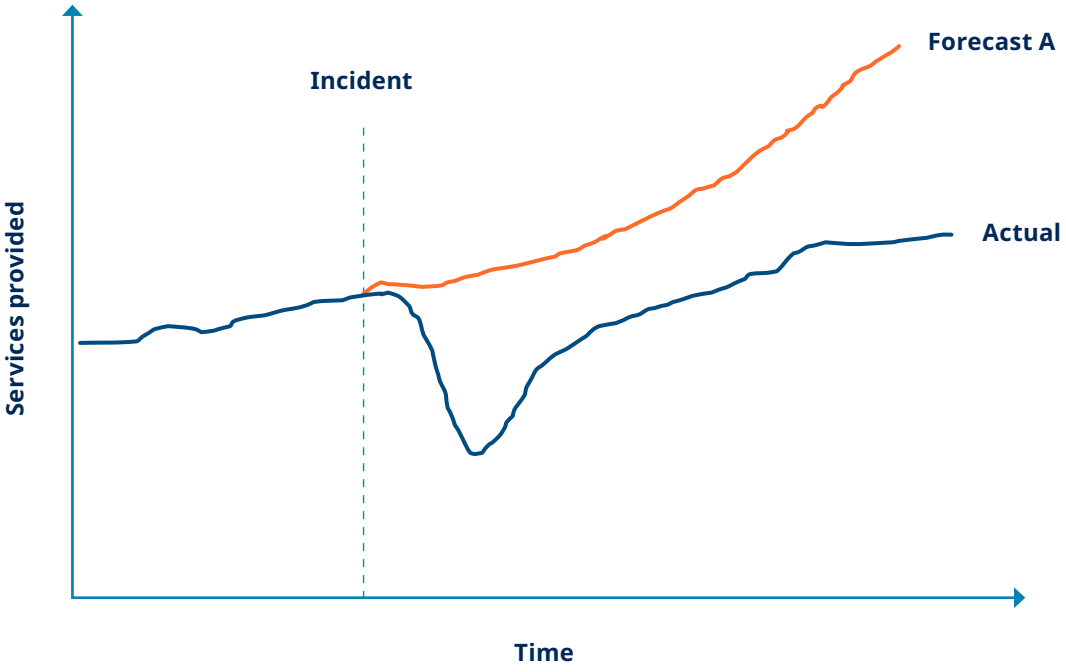


Figure 1: Schematic of a hypothetical impact of a cyber incident on an organisation

In evaluating the costs of a cyber incident, and the dynamic flow of costs, we would argue that it is important to take account of opportunity cost and evaluate costs relative to what could/would have happened without the attack. To illustrate, consider the hypothetical example in Figure 1 of the impact of a cyber incident on the services provided to clients by an organisation. Actual provision (see the 'Actual' line in Figure 1) declines as a consequence of the incident and then recovers over time to its former level. In measuring the cost of this decline, one crucial thing to consider is what would have happened without the incident. In Figure 1, we provide one scenario. Forecast A corresponds to a scenario in which there was predicted to be strong growth in service provision without the cyber incident. Actual provision is well below what would have been forecasted without the incident and the costs of the incident should take account of this loss relative to the forecast. Measured against the latest pre-incident level of service provision, this incident would instead appear neutral in terms of its long-term impact; an understatement of its true harms. It is also important to consider the cumulative damages arising from this incident, that is, the total loss comparing Forecast A and Actual post-incident, rather than simply comparing the difference at any one point in time.

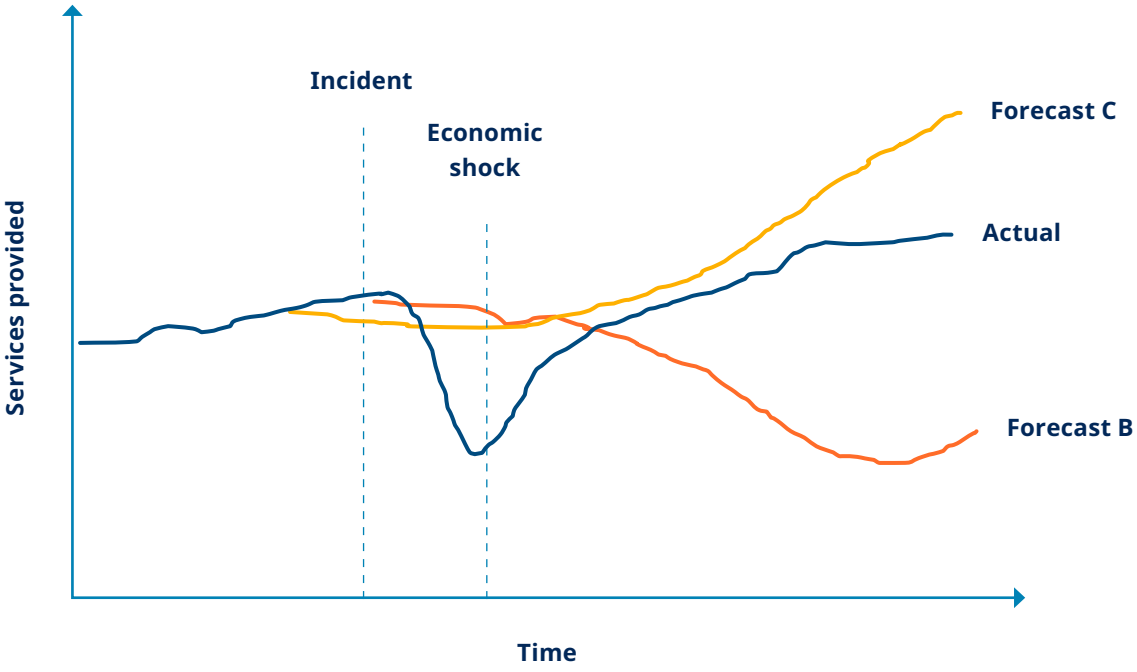


Figure 2: Schematic of a hypothetical impact of a cyber incident on an organisation

In Figure 2, we provide an alternative scenario. In this case, there is a negative shock that hits the economy after the cyber incident (e.g., COVID-19 or the Ukraine war), which negatively impacts the wider economy. Forecast B provides an interesting case in which service provision was forecasted to fall without the incident (because of the shock to the economy). In this scenario, the incident positively impacts the organisation by improving its readiness and resilience to the subsequent shock. The organisation is, therefore, better prepared for the shock than it would have been without the incident. At face value, such learning could be viewed as a 'benefit' of the cyber incident. Care, however, is needed in interpreting such benefits. In measuring the cost of a cyber incident, consideration must be given to what could or should have happened without the incident. If there was a lower-cost means for the organisation to have learnt lessons, then this should be the relevant comparator.

To illustrate, Forecast C in Figure 2 depicts an outcome in which the organisation improved resilience by implementing best practice guidance and learning from others. Under this scenario the organisation not only avoids the negative impact of the cyber incident but also is better placed to cope with the external shock. If it could reasonably have been expected for the organisation to have followed best practice, then Forecast C is the relevant comparator. Again, we see that, on this criteria, the cyber incident has a negative impact on the organisation. As this stylised example illustrates, care is needed in measuring the **costs and benefits that are attributable to the attack**. To give a practical example: If, as a consequence of an incident, an organisation migrates to the cloud and/or provides more staff training then these should not be considered costs if the organisation should have been doing them anyway. Similarly, if migration to the cloud and/or staff training increases productivity then these should also not be considered benefits.

Forecasting what would or should have happened in the absence of an incident is complex. Large organisations, however, routinely make medium to long-range forecasts on key business indicators and so the ability should exist to do hypothetical comparators. Also, note that estimates of cost can be updated with time and retrospective forecasting. This can improve estimates of, for instance, movements in share price or sales relative to that of comparator firms in the market. It is not unreasonable, therefore, to expect a model of costs to take account of opportunity cost. Markets can also provide a source of quantifiable information on the impact of a cyber incident relative to expectations. To give a specific example, if a firm is publicly listed, movements in that firm's share price can be used to infer the overall financial impact of an incident.

This financial impact includes both direct financial costs in the form of reductions in current and expected future profits, as well as indirect costs that ultimately have a financial implication for the firm, for example, future regulatory fines or anticipated lawsuits associated with harm suffered by its employees or customers. Tosun (2021) shows that an unanticipated cyber attack leads to higher trading volumes in the affected firm's shares due to selling pressure that ultimately reduces stock returns. Incidents can affect the targeted firm's strategies for up to five years after the attack, moreover. Interestingly, Tosun (2021) shows that, while abnormal excess returns drop by 100 basis points for targeted firms at the event date, the abnormal excess returns for (unaffected) control firms also drop, albeit by a lesser amount (60 basis points). This could be a consequence of the market perceiving those firms as being at increased risk and may also reflect the indirect economic spillover effects discussed in Deliverable 2 of this project. For a summary of related results, see Woods and Böhme (2021).

A further complexity in estimating the costs of a cyber incident is the consideration of intangible costs. Many costs of a cyber incident are intangible, e.g., reputation loss and psychological harm to managers and employees. It is essential that such costs should be accounted for. Fortunately, economics provides a practical roadmap to how intangible costs can be quantified in financial terms. As an example, the psychological harm from stress can be quantified by looking at sick leave and absence from the workplace (Wolvetang et al. 2022). Similarly, reputation loss can be measured by looking at reactions in share prices (Cannas et al. 2009, Tweneboah-Kodua et al. 2019) or increased interest rates from debt. The impact of DDoS attacks can be measured by trade volume (Abhishta et al. 2019). Such methods are currently underdeveloped in the analysis of cyber security incidents, so there is scope for more research exploring ways to measure intangible costs. Put differently, there is a need to move beyond a taxonomy of cyber harms and look to develop best practice methods of measuring the identified harms.

An Overview of Approaches for Assessing the Cost of Incidents

The expanding digital landscape has underscored the critical need for robust cybersecurity measures. As cyber threats evolve and target interconnected systems, the complexity of assessing the financial repercussions of security breaches increases. Traditional cost assessments, often rooted in probability-based simulations, face challenges in accurately reflecting the multifaceted nature of cyber risks. These simulations are a set of quantitative techniques that predict potential financial losses by calculating the likelihood of various cybersecurity events and their respective impacts. They often rely on statistical methods and risk analysis theories to forecast the fiscal consequences of cyber threats. They fail to capture complex harms, which may lead to further financial losses due to indirect reputational factors or long-term legal proceedings brought by customers and clients. They do, however, provide an effective baseline cost representing the costs associated with interruption of business and breaches of policy (in particular privacy regulations).

For example, Monte Carlo simulation (Linsmeier et al., 2000; Kavak et al., 2021), a widely used probability-based technique, generates a range of possible outcomes for a given cyber threat by simulating the random processes that could lead to that threat materialising and, subsequently, estimating the potential costs. Each run of simulation, employing random sampling, yields a unique set of results due to the inherent uncertainty and variability of cyber incidents. It provides, therefore, a way of generating different forecasts, such as those in Figures 1 and 2. Over many runs, these simulations provide a distribution of possible outcomes from which organisations can estimate the probability and impact of cyber incidents. Woods et al. (2021), and Woods and Simpson (2018) highlight the use of such statistical models in cybersecurity economics.

Despite the robustness of the Monte Carlo simulation, the technique is not without drawbacks. The simulation's reliability is contingent upon the quality and relevance of the historical data used. In cybersecurity, where the threat landscape evolves rapidly, historical data may not adequately predict future incidents. Emerging threats may not be represented in past data, and the complexity of digital environments can introduce novel variables that challenge the accuracy of traditional models. Furthermore, while these models provide a basic understanding of cybersecurity economics, they may not fully account for the distinct characteristics of different business environments or adequately consider the full spectrum of real-world cost factors. For instance, a financial institution that handles sensitive customer data may face higher regulatory compliance costs post-breach than a manufacturing company, which might face more significant operational disruptions and loss of proprietary information. Similarly, a tech start-up with cloud-based assets has different security concerns and potential cost implications compared to large companies with their own physical and digital infrastructures. Often, these models don't account for the different risks each sector bears, nor do they fully address the various direct and indirect costs stemming from cyber incidents. It's also important to consider the risk transfer - for instance, cloud providers like AWS may have policies that do not take responsibility for data protection in certain jurisdictions, leaving the risk with the user.

As previewed in the previous section, determining the cost of a cyber incident accurately requires a detailed breakdown of the cost components. Direct costs are immediately incurred following a cyber incident, including forensic investigations, legal ramifications, and remediation efforts. Indirect costs, often subtler and more protracted, involve organisational resources devoted to recovery efforts, such as internal communications, account reinstatements, and operational inefficiencies. Perhaps most damaging are the intangible costs, which manifest as diminished customer trust, erosion of brand reputation and subsequent loss of revenue. Additionally, for many larger organisations, the interruption of business may represent the most significant financial impact, potentially exceeding the costs of remediation itself (Romanosky at al., 2016; Kamiya et al., 2021; Romanosky et al., 2019).

The Value at Risk (VaR) concept, established by Linsmeier et al. (2000), is well recognised in economics as a framework for quantifying potential financial losses within a specific time frame and risk parameter. VaR, a benchmark in economic disciplines and financial institutions, captures the essence of risk measurement by estimating the maximum anticipated losses over a set period at a predetermined confidence level (Amaya et al., 2015; Cabedo et al., 2003; Duffie et al., 1997). It is predicated on the notion that by identifying and examining the critical variables affecting an asset's value, one can estimate the maximum potential loss for a designated period with a certain degree of confidence. This estimate is intrinsically linked to a probability threshold—expressed as the firm's potential loss over time 't' with a probability 'p' (Duffie et al., 1997; Guermat et al., 2002; Romanosky et al., 2016). VaR is typically computed using one of three primary methods: historical simulation, which uses the statistical distributions of past market changes; the delta-normal method, based on a presupposed multivariate normal distribution of risk factors; and Monte Carlo simulations, which, like historical simulations, generate scenarios based on probability distributions instead of relying solely on historical data (Linsmeier et al., 2000).

In stark contrast, the cyber domain is only beginning to fully integrate VaR into its risk assessment frameworks. Traditional cybersecurity risk assessments usually concentrate on the specific types of cyberattacks and their underlying motives, as depicted by the World Economic Forum and Deloitte (2015). This narrow focus is broadening to include a more holistic perspective that addresses all threats—adversarial and non-adversarial alike—as well as the assets at risk and their inherent vulnerabilities. Contemporary sources, such as the NIST SP 800-37 Rev. 2, indicate a move towards integrating newer risk quantification methods that align with current standards and practices in cybersecurity, reflecting a bridge between academic insight and operational implementation (NIST 2018).

The World Economic Forum emphasises that a comprehensive cyber-risk model should incorporate the assets at risk, the profiles of potential attackers, and system vulnerabilities to achieve a holistic loss distribution that captures all potential threats (World Economic Forum and Deloitte, 2015). Such a model would extend beyond merely tallying post-breach costs to proactively anticipating the financial impact of cyber threats. While the Forum details the considerations for such a model, there remains an ongoing debate within academic and professional circles over the most effective approach to its development. Some propose that, in addition to traditional risk factors, the model should integrate controls as dynamic variables that affect risk—such as intrusion detection systems, automated security patching, and advanced encryption—which directly influence the likelihood and severity of threats materialising (Böhme et al., 2018; Eling et al., 2019). Alternatively, Erola et al. (2013) suggest data schemas that blend estimates of digital assets' value with classifications of cyber incidents (Ruan et al., 2017; Dieye et al., 2020), advocating for a more detailed and data-centric approach to Cyber Value at Risk (CVaR).

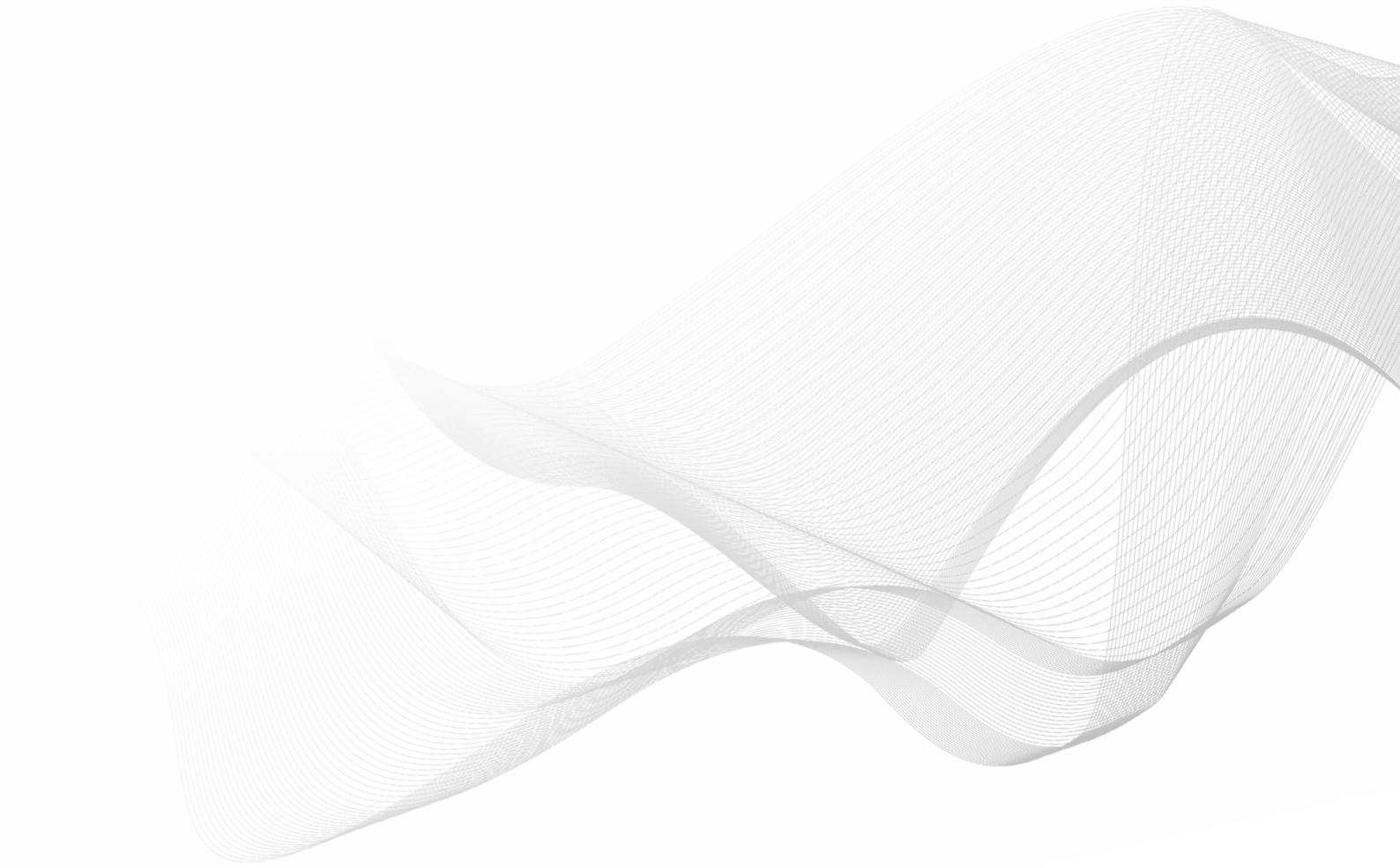
List of Models and Approaches	Description
Value at Risk (VaR)	A well-established method in finance, used to benchmark trading portfolios and assess market risk exposure. Regulators also recognise VaR as a quantitative measure for information disclosure.
Cyber Value at Risk (Cyber VaR)	It is an adaptation of VaR for the cyber domain. It estimates the maximum potential loss an organisation could face over a specified period at a given probability level.
Historical Simulations	Utilizes historical data to simulate past variations in asset values to identify potential future fluctuations.
Delta-Normal Approach	Presumes that risk factors follow a multivariate normal distribution and calculates VaR based on the correlations among these factors.
Monte Carlo Simulations	Similar to historical simulations but employs generated scenarios informed by probability distributions, not solely on past data.
Parametric Models	Designed to account for market changes, predicated on assumptions of normality, serial independence, non-linearity, skewness, kurtosis, and volatility in variables.
Exponentially Weighted Moving Average (EWMA)	Tackles scenarios where time-series data volatility impacts VaR computations.
Generalized Autoregressive Conditional Heteroskedasticity (GARCH)	Addresses kurtosis irregularities within time-series data for more accurate VaR estimation.
Actuarial Science Methods	Applied to cyber-attack datasets to deduce VaR.
Factor Analysis of Information Risk (FAIR)	Incorporates Bayesian networks to model diverse loss distributions and the dynamics between attackers and defenders.
VERIS Community Database	Aims to document cyber incidents and their consequences comprehensively.
Advisen Loss Dataset	Analogous to VERIS, compiles cyber incident data for analytical use.
Risk Management Solutions (RMS) and Cambridge Centre for Risk Studies Schema	Takes an insurer-centric view, correlating assets, controls, cyber harms, and threats.
Applied Insurance Research (AIR) Schema	Offers asset options and considers data transfer and quality standards, associating specific data with insurance policies.

Table 1: Summary of Existing Models and Approaches for Assessing Cyber Incident Costs

The burgeoning field of Cyber Value at Risk (CVaR) represents a significant shift in risk quantification, capturing the maximum potential loss an organisation could face over a specified period due to a cyber attack within a given probability threshold. CVaR is not a single estimate but a distribution considering a range of potential outcomes and their respective probabilities. This approach recognises the entire spectrum of risk rather than just the extremes.

However, the transition from traditional VaR to CVaR is not simply a reapplication of financial concepts to the realm of digital security; it is necessitated by the distinctive characteristics of cyber risks. Unlike static market variables, cyber threats are dynamic, evolving rapidly, with new risks emerging before previous ones are fully understood or even identified. As such, while traditional financial VaR models benefit from historical market data, CVaR must contend with often less predictable and quantifiable factors (Orlando et al., 2021; Erola et al. 2022; University of Oxford. 2020).

Erola et al. (2022) proposed a conceptual framework to calculate CVaR using Monte Carlo simulations, enabling organisations to gauge residual risk from cyber incidents, even with existing security controls in place. Key parameters utilised in their model to assess CVaR are outlined in Table 2. Their paper details the successful application of this CVaR model in a real-world case study, demonstrating its efficacy in accurately predicting financial losses from cyber incidents and aiding professionals in assessing the impact of security measures and threat scenarios. However, the model's effectiveness depends heavily on the availability and quality of the input data, with noted limitations such as the need for more empirical data for ascertaining threat probabilities and control effectiveness, alongside the preliminary reliance on external data sources. These limitations underscore the urgent need for enhanced data collection and sharing practices within the cybersecurity community to refine the model's accuracy and practical application.



Key Parameters	Description
Assets	The value of the assets at risk, which may include physical devices, data, software, people, and organisational processes, requires an assessment of their replacement or economic value to the organisation.
Threats	The likelihood of different cyber threats materialising, which target the identified assets. This includes a detailed analysis of potential cyber-attacks and their frequency.
Controls	The suite of risk controls in place to protect the assets reflects their associated residual risk, encompassing the presence and effectiveness of these measures, often categorized qualitatively (e.g., high, medium, low).
Harms	Types of losses from cyber threats, or cyber harms, include direct costs like forensic investigations and remediation, as well as indirect costs such as lost opportunities and reputational damage.
Harm Propagation	The model accounts for the interconnectedness of harms, recognizing how one incident can catalyse further damage, thus amplifying the impact.
Probability Functions	These are used to estimate the likelihood of occurrence and the effectiveness of controls for each threat, control, and harm identified.
Value at Risk	The model calculates the maximum potential loss an organisation could face over a period due to a cyber-attack, quantified at a given probability level.
Monte Carlo Simulations	Employed by the model, these simulations generate a range of possible outcomes for cyber threats by mimicking the random processes that could lead to their realization.
Loss Distributions	Different probability distributions are used to estimate the CVaR, significantly influencing the outcome based on the choice of distribution (e.g., normal, log-normal).
Effectiveness of Controls	Data on how effectively the controls mitigate risks is required, which could come from historical performance data or industry benchmarks.
Insurance Premiums	This considers information on past insurance claims and pricing to deduce the potential costs associated with cyber incidents (Pal et al., 2017).

Table 2: Key parameters in the CVaR Model proposed by Erola et al. (2022)

Franco et al. (2024) recently proposed another approach, the Real Cyber Value at Risk (RCVaR), which offers an economic estimation of potential financial losses from cyber incidents affecting various companies. This estimation leverages data drawn from public cybersecurity industry reports published by major consulting companies, such as Accenture (Bissell, K et al., 2019; Bissell K et al., 2021), IBM (IBM Corporation., 2022), Ponemon Institute (Ponemon Institute LLC., 2012) and Kaspersky (Kaspersky Lab ZAO., 2013.). The authors identified and summarised several significant cyber risk factors in Table 3 to aid in estimating the costs associated with cyber incidents.

Cyber Risk Factors	Description
Industry Sector	Different industries encounter varying levels and types of cyber threats due to their unique operational practices, data sensitivities, and regulatory environments, making the industry sector a significant determinant in assessing the likelihood and potential impact of cyber incidents.
Company Size	The size of a company, often gauged by revenue, employee count, or market capitalisation, influences its cyber risk profile. While larger companies may be more appealing targets for cybercriminals, they may also possess stronger cybersecurity defences.
Geographic Location	A company's geographic location can impact its exposure to cyber risks, influenced by regional variations in cyber threat landscapes, legal and regulatory frameworks, and the prevalence of specific cyberattack types.
Type of Cyber Incidents	Various cyber incidents, such as data breaches, ransomware attacks, and phishing scams, entail different cost implications, with the incident's nature significantly affecting the direct and indirect costs incurred.
Security Measures in Place	An organisation's cybersecurity measures and policies are crucial in risk mitigation. Companies with sophisticated security technologies and practices are likely to incur lower costs from cyber incidents.
Number of Employees	A company's employee count may indicate the scale of its network and potential attack surface, as well as the overall level of cybersecurity awareness and training among the workforce.
Cloud Model	A company's adoption of cloud services and the choice of cloud deployment model—public, private, or hybrid—can shape its vulnerability to cyberattacks and related costs.
Employee Training	Cybersecurity awareness and training programs for employees are pivotal in reducing the risk of human-error-induced incidents, a notable cause of many cyberattacks.
Percentage of Remote Employees	The rise in remote work has implications for a company's cyber risk profile, as a higher percentage of remote employees may introduce new vulnerabilities.
Cyber Insurance	A company's cyber insurance coverage can significantly influence the financial impact of a cyber incident, making it a critical factor in risk management.
Multi-factor Authentication and Identity Access Management	Implementing multi-factor authentication and robust identity access management systems can substantially lower the risk of unauthorised access, thereby mitigating potential costs.

Table 3: Identify Key Risk Factors for Estimating the RCVaR Across Different Companies

Martin et al. (2018) present an alternative method for calculating the cost of cyber incidents, employing actual cost data from an operational risk database, encompassing a wide array of cyber incidents, not limited to data breaches. Similarly, Meurs et al. (2022) examined the payment and financial loss of ransomware attacks based on data given to the Dutch police.

A thorough review of various methods to assess cyber incident costs reveals that no singular model provides an absolute solution, given the complex and evolving nature of cyber threats. Classical approaches, including Monte Carlo simulations and other probability-based methods, have established the foundational principles for the financial quantification of cyber risks. However, these models are increasingly challenged by the rapid evolution and unique complexities of the cyber threat landscape, leading to potential inaccuracies when relying solely on historical data. As we discuss shortly below, such methods only capture some of the harms from cyber incidents.

The adaptation of Value at Risk (VaR) to Cyber Value at Risk (CVaR), and further to Real Cyber Value at Risk (RCVaR), signifies a notable progression towards more sophisticated, forward-looking models that aim to encapsulate the full spectrum of cyber risk factors. These models strive to rectify the limitations of traditional simulations by considering a more comprehensive array of variables, including industry-specific threats, organisational cybersecurity posture, and the swift evolution of cyber threats. Additionally, the Factor Analysis of Information Risk (FAIR) model, incorporating Bayesian networks, furnishes a refined framework to examine the interplay between attackers and defenders, heralding a promising avenue for future research and application.

The FAIR approach, one of the most prominently referenced quantitative risk assessment frameworks (see Deliverable 1 on cyber quantification systematic literature analysis). This methodology centers on the assets susceptible to risk and delineates categories of threat communities, encompassing insiders, cyber criminals, or malware. Attributes such as motivation, expertise, and potential collateral damage are additionally factored into the analysis (Ekstedt et al. 2023). Figure 3 elucidates the sequential calculation steps integral to the FAIR approach (Wang et al. 2020). Despite being among the methodologies that emphasise risk assessment and quantification, boasting a high degree of comprehensiveness compared to others (Wangen et al. 2018), this diagram underscores a fundamental challenge shared by many risk assessment models: their reliance on historical data (Jouini and Rabai 2016).

Given the sequential nature of calculations within FAIR, inaccuracies at any stage can reverberate throughout subsequent computations. A wealth of data is necessitated to ascertain parameters such as loss frequency, event frequency, and loss magnitude. This entails comprehensive datasets encompassing various threat categories, including malware, phishing, data breaches, DDoS attacks, zero-day exploits, insider threats, ransomware, social engineering, and supply chain attacks. Moreover, data about financial aspects are imperative, including fines associated with cyber incidents, expenses incurred for engaging experts or legal counsel, data and hardware recovery costs, quantification of reputational damage, and valuation of compromised data (Lee 2021). Additionally, insights into attacker motivation, recurrence rates of subsequent attacks on the same target, and perpetrators' post-ransom payment behavior are invaluable for accurate risk assessment.

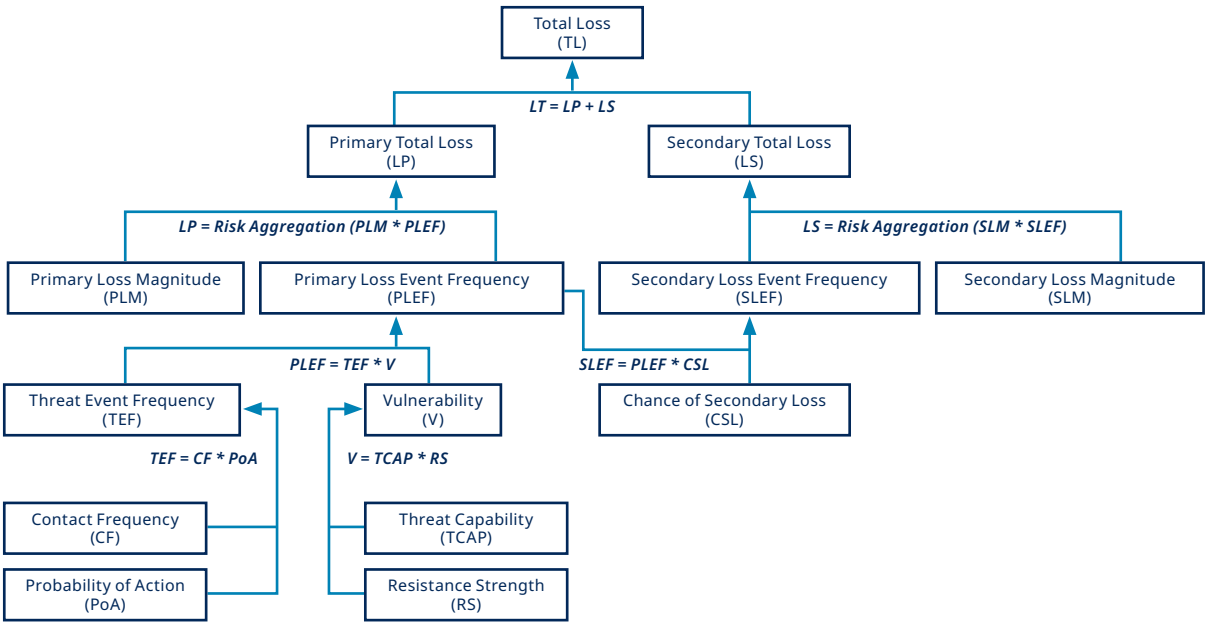


Figure 3: Sequential calculation steps in FAIR

The current trend points to a hybrid approach that combines the strengths of various methodologies, supplemented by rigorous data collection and sharing practices, to enhance the precision and utility of cyber incident cost assessments. Models that factor in the unique attributes of each organisation, such as asset value, industry sector, size, geographical location, and the type and effectiveness of security measures, are emerging as the front-runners in this domain. We finish, however, by highlighting that existing approaches are primarily focused on financial costs and so are not capturing many of the harms we know are important in cyber incidents, most notably psychological costs. There is no reason why approaches such as VaR could not incorporate psychological harms but that requires accurate data. A danger with approaches such as VaR, therefore, is that they focus on costs, typically direct tangible costs, for which there is more data available.

The Pros and Cons of Quantifying Incidents

An essential component of cyber risk management involves determining the appropriate response to identified risks and optimising the allocation of the organisation's resources within this framework. A pivotal tool in this endeavour is cost-benefit analysis, which requires the valuation of acceptable risks. Individual risks are evaluated for this process, and determinations are made regarding the degree to which they should be mitigated, eradicated, or accepted. Moreover, considerations extend to whether risks are managed internally within the organisation, such as through investments in IT infrastructure or human resources, or whether risk transfer mechanisms, such as cyber insurance, are employed. Accordingly, a viable strategy may involve a blend of risk mitigation measures and insurance provisions aimed at minimising risks to an acceptable threshold in a cost-effective manner (Gordon et al. 2003; Bandyopadhyay and Mookerjee 2019).

As previously highlighted within the scope of this study, risk assessment methodologies are categorised into qualitative and quantitative approaches. Qualitative methods facilitate the prioritisation of risks by assigning weightings and utilising methodologies such as the Analytic Hierarchy Process (AHP) or other Multi-Criteria Decision Making (MCDM) techniques. However, these methods do not yield quantifiable values, thus complicating the integration of such assessments into cost-benefit analyses (Bhattacharjee et al. 2013). Moreover, qualitative risk assessment models often yield subjective and variable outcomes regarding potential losses, as they lack grounding in mathematical or statistical observations. Conversely, quantitative risk assessment methods furnish an objective and consistent foundation for analysis, rendering them particularly apt for incorporation into cost-benefit evaluations (Meriah and Rabai 2018). These methods, however, rely on the accuracy of data.

At a more general level, in order to assess the advantages and disadvantages of costing cyber incidents, we have to be clear about the scope of the quantification exercise that is being carried out. In particular, while broadening the scope (quantifying a wider range of costs) can lead to new benefits, it may also generate new limitations in terms of how accurately those costs can be measured. As discussed above, the costs that may conceivably be included within the scope of the costing exercise differ in terms of:

- The *nature* of the cost (financial, reputational, psychological, physical, etc.)
- The *bearer* of the cost (the initial target, the Exchequer, a supplier of the target, a customer, an employee, etc.)
- The level of *aggregation* in terms of both:
    - The target of the attack: are we considering the cost of an incident at an individual firm or the consequences of a sector-wide attack, and
    - The bearers of the associated costs: are we considering the impact of a given incident on one firm or a sector, on one employee or a firm's IT department, on one customer or a market of consumers
- The *timeframe* over which these costs accrue

It is also important to consider who the beneficiary or end user of the costing information is. This beneficiary may differ from the firms/people who bear the costs in question. For example, a government might be interested in the psychological harms suffered by a group of employees, and a firm might care about the physical harm its employees suffer as a result of burnout (not least because some of these physical costs might ultimately translate into financial costs for the firm, see below). The advantages and disadvantages of costing incidents may differ, depending on who the end user is. For example, using measures of accounting cost to quantify financial losses might be more useful for insurers than for firms and other end users that may want to consider a wider notion of economic costs.

ADVANTAGES OF QUANTIFYING INCIDENTS

- Quantifying cyber incidents provides an objective and comparable measure of the costs of cyber breaches. This estimate should always be understood in terms of the scope of the quantification exercise: it should be clear which costs are being estimated and which costs are not being considered. Similarly, cost estimates should be clear in terms of their unit of measurement (cost in sterling per incident, cost in sterling per year, cost in terms of days of sick leave by employees, etc.). This ensures that comparisons are made only between cost estimates that are truly comparable.

- Firms can benefit from costing cyber incidents to improve the quality of their decision making in terms of which areas of vulnerability to focus on. Clear cost estimates can facilitate communication with senior management, shareholders and others in the complex area of cyber-risk mitigation. Quantifying costs can also help firms to assess the effectiveness of mitigation strategies in terms of how much they reduce the costs of particular cyber attacks. Finally, costing cyber incidents may confer a competitive advantage on firms by helping them to avoid business strategies that expose them to excessive cost and by encouraging cybersecurity best practices that reduce their exposure relative to rival firms (Amin 2019).

- In quantifying the financial cost of an incident, it is important for firms to consider hidden costs such as increases in the cost of insurance, increases in their cost of capital, lost customer relationships and losses of intellectual property (Deloitte 2016). It is also important to bear in mind that costs that are initially non-financial in nature, e.g. psychological and physical costs suffered by employees and customers, can translate into financial costs to the firm in the form of increased staff absence and litigation. For clarity and comparability, any costing exercise should therefore be clear about the scope of the financial costs that it is considering.

- Aggregating the financial costs of an incident across the economy can allow implications about industry profitability (the tax base) and thereby predicted tax revenue to be derived. This aggregation exercise must take care of the aggregation issues discussed in Deliverable 2 of this project, in particular the fact that financial costs arising at one firm may be amplified or mitigated as the effects of an attack spread through the economy.

- For governments and regulators, costing cyber incidents can allow for damages that extend beyond the immediate financial harm of an incident to be quantified. While financial costs may be most relevant to individual firms, from a societal point of view, a broader range of costs including psychological costs, potentially arising over a longer timeframe, can be relevant. This includes psychological costs that go beyond those that can ultimately be transferred to firms, moreover (see previous point). Government and regulators may be particularly interested in costings at a higher level of aggregation.
- Accurate cost estimates of an appropriate scope can allow cost-benefit analyses of new cybersecurity programmes and initiatives to be carried out.
- If psychological and other costs are found to be important but are not fully incorporated in the costing exercise carried out by firms, regulatory interventions to bring firms' private cost estimates more closely into line with society's priorities could be explored.
- For both firms and governments/regulators, developing clear and comparable costing methodologies can reduce the reliance on cost estimates provided by vendors of security services and technologies, which may overestimate the costs of cyber-incidents for strategic reasons (Woods and Böhme 2021).

DISADVANTAGES OF QUANTIFYING INCIDENTS

The disadvantages of costing incidents arise as a result of technical and informational constraints that mean accurate cost estimates may be difficult to obtain. There is likely to be a trade-off between the scope of the costing exercise on the one hand and the accuracy and comparability of the results obtained, as well as the administrative burden that implementing the costing model imposes on firms, on the other. These considerations therefore influence the design of a standard model of costing incidents that we turn to in the following section.

- Quantifying the cost of cyber incidents is likely to be simpler if attention is restricted to financial costs. Even in this respect, there are several issues that need to be considered. These include the distinction between accounting costs and economic costs. Accounting costs, as reflected in the amortised book value of assets, for example, are simpler to obtain and may be particularly relevant for insurance firms.

- The concept of opportunity cost provides a broader notion of what constitutes relevant financial costs in connection with a cyber incident. For example, if a firm needs to purchase new computers as a result of a cyber attack, but was in the process of updating its computing infrastructure anyway, the opportunity cost of the new computers should be negligible. As discussed above, measuring opportunity costs is complex because it requires an assessment to be made of the possible courses of action that could have been taken, had the incident in question not taken place. Managing the comparability issues that can arise in connection with opportunity costs requires clear guidance to be given to firms on how these costs should be measured (for example, this might require tangible evidence about actions that were planned and approved before the incident took place).

- The psychological and physical costs of an attack may be quantified, either in terms of their impact on the individual(s), or in terms of their contribution to the overall financial costs suffered by a firm (see above). In either case, care needs to be taken to measure these effects accurately. If we use staff absences as our measure of psychological or physical ill health, for example, we need to know, not only the number of recorded staff absences following an incident, but also the likely number of absences that would have occurred without the cyber incident (in the counterfactual). In this way, we can quantify the additional absences that are attributable to the incident in question. This can be managed in practice by comparing observed staff absences with information on past staff absences in a comparable period, for example. This should avoid the most significant measurement errors without introducing excessive complexity.

- Quantifying physical and psychological costs may require us to translate them into common units of measurement (say sterling). This is especially true if these costs are being aggregated with costs of another nature, e.g. financial costs, which are measured in sterling. This requires complex assumptions to be made regarding the value of human health. It is notable that the NHS did not calculate the total financial impact of cancelled appointments in connection with the 2017 WannaCry attack (National Audit Office 2018). The same is true of press reporting into the costs of the 2020 attack on Hackney Council, which did not attempt to quantify the costs of disruptions to services (UKAuthority 2022). Arguably, measuring psychological and physical costs should be easier if we are considering their financial impact on the employing firm rather than on the affected individuals.

- The quantification exercise becomes more complex, the longer the timeframe over which relevant costs are estimated. To quantify the longer term financial costs of an incident, for example, as discussed above, we need to forecast the flow of profits after an incident has occurred and compare these with the likely path that profits would have taken in the absence of the attack. Adopting an upper limit on the timeframe within which costs should be estimated can mitigate these complexities and promote the comparability of cost estimates. This approach can be justified since discounting future costs by a suitable discount factor (interest rate) implies that future costs weigh less heavily in today's decision than do current costs. In practice, business forecasts that were made before the incident took place should represent a useful snapshot of the likely counterfactual. These forecasts can then be compared with updated predictions that are made after the incident.

- As discussed above, behavioural and learning effects are relevant in costing incidents. While a given cyber-breach might generate a cost for a firm, it may also generate behavioural changes that lead to improved security practices and lower cyber costs in future. While this would tend to lower the cost of cyber incidents, it is important to consider here the extent to which the behavioural changes in question can be induced without a cyber-attack taking place. That is, to what extent is the benefit attributable to the incident and not associated with a feasible, less harmful alternative? To avoid excessive complexity in the costing exercise, these learning effects should be incorporated only where there is no conceivable alternative policy or scenario that could have generated those benefits.

- Firm behaviour is influenced by the market context. The incentives that firms face to adopt secure behaviours and therefore the costs of an attack on those firms are influenced by the availability and design of cyber-insurance contracts, for example. The standard moral hazard result predicts that insured firms are less incentivised to protect against the costs of cyber-attacks, though empirical evidence on this point is weak (Arce et al. 2024, Khalili et al. 2020, Woods and Moore 2020). The standard adverse selection result predicts that only the highest risk firms will end up purchasing insurance. Using incidence response panels that randomly assign incident-response service providers to firms can mitigate the adverse selection problem by attracting policyholders with lower expected losses, however (Arce et al. 2024).

- The above complexities are likely to be exacerbated to the extent that we move beyond costing an incident that has already occurred (backward-looking quantification) to costing future breaches (forward-looking quantification). Nevertheless, many of the benefits associated with an improvement in a firm's security practices or a new cybersecurity programme or policy are likely to arise in the form of reductions in the expected cost of future incidents. Developing a clear approach to quantifying past incidents is likely to be the most useful first step in quantifying future scenarios.

Key Recommendations

Our key findings can be summarised:

1. There exist evidence based taxonomies of cyber harms that provide a good framework for estimating the cost of a cyber incident. Such taxonomies cover a wide range of costs including psychological and societal harms.
2. There are well established methods to estimate the costs of a cyber incident, using and building upon a value at risk approach. It is not clear, however, to what extent such methods currently capture all of the harms from an incident or take into account opportunity cost and attributable costs.
3. Building on existing approaches, particularly in terms of costing of intangible loss, we believe it is feasible to develop a standard model of costing a cyber incident that would be applicable to most organisations and types of cyber incident.

Our key recommendations for a standard model of costing a cyber incident can be summarised:

1. A standard model needs to take into account the desired output of the user. For instance, the needs of a business or insurer in costing an incident may be very different to those of a government department or regulator. The scope of the costing exercise should be clear, e.g., whether social or spillover costs are included.
2. The model needs to take account of intangible as well as tangible costs, e.g., psychological costs to staff impacted by the incident and loss of reputation to the firm.-Various economic approaches exist to quantify intangibles, e.g. using loss of productivity and/or loss of staff time due to sickness as measures of psychological impact.
3. The model should be clear and transparent in the assumptions used to cost the incident, e.g. discount rate, calculation of downtime and calculation of staff time, as well as methods, e.g., accounting versus economic cost. The model should be flexible to allow for different underlying assumptions, e.g., estimating the cost of the incident for different values of the discount rate.
4. The model needs to recognise the long run costs of a cyber incident. The long run costs of an incident (e.g., reputation loss) are difficult to quantify in the short run. The model needs, therefore, to allow for updates over time as new information becomes available.
5. The model should provide clear guidance on how to calculate the cost and, crucially, outline the data required to input into the calculation exercise. The organisation should perform mock exercises to verify that they would be in a position to capture the data required to calculate the cost of an attack. An evaluation of costs needs to have input from across the organisation, including IT, finance, HR and senior management.
6. A cyber incident can have 'benefits' for an organisation, particularly in terms of 'learning from experience'. However, these benefits should typically not be included in a costing of the cyber incident. Instead, the notion of opportunity cost should be invoked with a focus on attributable costs and whether the organisation could have 'learnt from experience' without the attack. In most instances there are resources and information that could have enabled the organisation to improve their cyber security and would have been less costly than a cyber attack.
7. The model should reflect the resources and capabilities of the organisation to perform the exercise. For example, a small businesses will have less capability to perform a complex costing exercise. Crucially, the model should not seek simplification by narrowing scope because intangible losses (e.g., psychological stress) are particularly relevant for small organisations. Instead, the model needs to provide sufficient guidance and support to be simple to implement.

References

Abhishta, A., Joosten, R., Dragomiretskiy, S., & Nieuwenhuis, L. J. (2019). Impact of Successful DDoS Attacks on a Major Crypto-currency Exchange. In 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP) (pp. 379-384). IEEE

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A Taxonomy of Cyber-harms: Defining the Impacts of cyber-attacks and Understanding How They Propagate. Journal of Cybersecurity, 4(1), tyy006

Alohali, M. 2019. A Model for User-centric Information Security Risk Assessment and Response (Doctoral dissertation, University of Plymouth)

Amaya, D., Christoffersen, P., Jacobs, K., & Vasquez, A. (2015). Does Realized Skewness predict the cross-section of equity returns? Journal of Financial Economics, 118(1), 135-167.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the Cost of Cybercrime. The Economics of Information Security and Privacy, 265-300

Arce, D., Woods, D. W., & Böhme, R. (2024). Economics of incident response panels in cyber insurance. Computers & Security, 140, 103742. https://doi.org/10.1016/j.cose.2024.103742

Bandyopadhyay, T. and Mookerjee, V. (2019) 'A Model to Analyse the Challenge of Using Cyber Insurance', Information Systems Frontiers, 21, 301-325

Bhattacharjee, J., Sengupta, A. & Mazumdar, C. (2013) 'A Formal Methodology for Enterprise Information Security Risk Assessment'. In 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS), IEEE, 1-9

Bissell, K., & Ponemon, L. (2019). The Cost of Cybercrime. Accenture Security

Bissell, K., J. Fox, R. M. LaSalle, & et al. (2021). How Aligning Security and the Business Creates Cyber Resilience

Böhme, R., Laube, S., & Riek, M. (2019). A Fundamental Approach to Cyber Risk Analysis. Variance, 12(2), 161-185

Cabedo, J. D., & Moya, I. (2003). Estimating Oil Price 'Value at Risk' Using the historical simulation approach. Energy economics, 25(3), 239-253

Cannas, G., Masala, G., & Micocci, M. (2009). Quantifying Reputational Effects for Publicly Traded Financial Institutions. Journal of Financial Transformation, 27, 76-81

Carfora, M., Martinelli, F., Mercaldo, F., & Orlando, A. (2019). Cyber risk management: An actuarial point of view. Journal of Operational Risk, 14(4)

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. (2023). How Cyber Insurance Influences the Ransomware Payment Decision: Theory and Evidence. The Geneva Papers on Risk and Insurance-Issues and Practice, 48(2), 300-331

Dart, M., & Ahmed, M. (2023). Operational Shock: A Method for Estimating Cyber Security Incident Costs for Large Australian Healthcare Providers. Journal of Cyber Security Technology, 1-26

Deloitte (2016). Seven Hidden Costs of a Cyberattack. Deloitte CFO Insights, July 2016. Available at: https://dart.deloitte.com/USDART/pdf/50783a6d-55a5-11e6-ba39-77e9a652f270

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the Macroeconomic Costs of Cyber attacks. Risk Management and Insurance Review, 23(2), 183-208

Devos, J.G., Munteanu, A. and Fotache, D. (2015) 'How Much Matter Probabilities in Information Security Quantitative Risk Assessment?'. Available at SSRN 2579624

Duffie, D., & Pan, J. (1997). An overview of value at risk. Journal of derivatives, 4(3), 7-49

Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S. and Lagerström, R. (2023) 'Yet another cybersecurity risk assessment framework'. In International Journal of Information Security, 22(6), 1713-1729

Eling, M., & Wirfs, J. (2019). What Are the Actual Costs of Cyber Risk Events? European Journal of Operational Research, 272(3), 1109-1119

Erola, A., Agrafiotis, I., Nurse, J. R., Axon, L., Goldsmith, M., & Creese, S. (2022). A System to Calculate Cyber Value-at-Risk. Computers & Security, 113, 102545

Franco, M. F., Künzler, F., von der Assen, J., Feng, C., & Stiller, B. (2024). Rcvar: An Economic Approach to Astimate Cyberattacks Costs Using Data from Industry Reports. Computers & Security, 139, 103737

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) 'A Framework for Using Insurance for Cyber-risk Management'. In Communications of the ACM, 46(3), 81-85

Guermat, C., & Harris, R. D. (2002). Forecasting Value at Risk allowing for time variation in the variance and kurtosis of portfolio returns. International Journal of Forecasting, 18(3), 409-419

Haji, S., Tan, Q. and Costa, R.S. (2019) 'A Hybrid Model for Information Security Risk Assessment', Internation Journal of Advanced Trends Computer Science. Engineering. (ART-2019-111611)

IBM Corporation. (2022). Cost of a Data Breach Report. Available at: https://www.ibm.com/security/data-breach

Jouini, M. and Rabai, L.B.A. (2016) 'Comparative Study of Information Security Risk Assessment Models for Cloud Computing Systems'. Procedia Computer Science, 83, 1084-1089

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. Journal of Financial Economics, 139(3), 719-749

Kaspersky Lab ZAO. (2013). Global Corporate IT Security Risks: 2013. Available at: https://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, 7(1), tyab005

Lee, I. (2021) 'Cybersecurity: Risk Management Framework and Investment Cost Analysis', Business Horizons, 64(5), 659-671

Linsmeier, T. J., & Pearson, N. D. (2000). Value at risk. Financial Analysts Journal, 56(2), 47-67

MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J. R., Turner, S., & Pattnaik, N. (2024). Ransomware: Victim Insights on Harms to Individuals, Organisations and Society

Meriah, I. and Rabai, L.B.A. (2018) 'A Survey of Quantitative Security Risk Analysis Models for Computer Systems'. In Proceedings of the 2nd International Conference on Advances in Artificial Intelligence, 36-40

Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). Ransomware: How Attacker's Effort, Victim Characteristics and Context Influence Ransom Requested, Payment and Financial Loss. In 2022 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-13). IEEE

National Audit Office (2018). Investigation: WannaCry Cyber Attack and the NHS. HC 414 Session 2017-2019. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

NIST (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

Orlando, A. (2021). Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. Risks, 9(10), 184

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2017). Security Pricing as an Enabler of Cyber-Insurance: A First Look at Differentiated Pricing Markets. IEEE Transactions on Dependable and Secure Computing, 16(2), 358-372

Ponemon Institute LLC. (2012). Cost of Cyber Crime Study: United States. Available at: https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity, 2(2), 121-135

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?. Journal of Cybersecurity, 5(1), tyz002

Ruan, K. (2017). Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk. Computers & Security, 65, 77-89

Tosun, O.K. (2021). Cyber-attacks and Stock Market Activity. International Review of Financial Analysis, 76, 101795

Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of Cyberattacks on Stock Performance: A Comparative Study. Information & Computer Security, 26(5), 637-652

UKAuthority (2022). Hackney Council Aligns Cyber Recovery with Modernisation. https://www.ukauthority.com/articles/hackney-council-aligns-cyber-recovery-with-modernisation/

University of Oxford and Axis (2020). White Paper: Calculating Residual Risk Cyber-Risk

Wang, J., Neil, M. & Fenton, N. (2020) 'A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR model', Computers & Security, 89, 101659

Wangen, G., Hallstensen, C. and Snekkenes, E. (2018) 'A Framework for Estimating Information Security Risk Assessment Method Completeness: Core Unified Risk Framework, CURF', International Journal of Information Security, 17, 681-699

Wolvetang, S., van Dongen, J. M., Speklé, E., Coenen, P., & Schaafsma, F. (2022). Sick Leave Due to Stress, What Are the Costs for Dutch Employers?. Journal of Occupational Rehabilitation, 32(4), 764-772

Woods, D., & Simpson, A. C. (2018). Monte Carlo Methods to Investigate How Aggregated Cyber Insurance Claims Data Impacts Security Investments

Woods, D. W., & Böhme, R. (2021, May). SoK: Quantifying Cyber Risk. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 211-228). IEEE

Woods, D. W., Moore, T., & Simpson, A. C. (2021). The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices. Digital Threats: Research and Practice, 2(2), 1-21

World Economic Forum and Deloitte (2015). Partnering for Cyber Resilience Towards the Quantification of Cyber Threats

Zambon, E., Etalle, S., Wieringa, R.J. and Hartel, P., 2011. Model-based Qualitative Risk Assessment for Availability of IT Infrastructures. Software & Systems Modeling, 10, pp.553-580

Zeller, G., & Scherer, M. (2022). A Comprehensive Model for Cyber Risk Based on Marked Point Processes and Its Application to Insurance. European Actuarial Journal, 12(1), 33-85

Zhang, Y., Wang, L., Liu, Z., & Wei, W. (2020). A Cyber-insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks. IEEE Transactions on Information Forensics and Security, 16, 1855-1867