OLIVER WYMAN

NAVIGATING CYBER RISK QUANTIFICATION

THE ART AND SCIENCE OF CYBER QUANTIFICATION THROUGH A SCENARIO-BASED APPROACH

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

QUANTIFICATION

A directional guide to effective risk management

Despite the increasing importance of cyber risk agenda within organisations, very few have a comprehensive understanding of their cyber risk exposure, making it difficult for organisations to effectively manage cyber risk. Quantification of cyber risk would help organisations deep dive into understanding their exposure and provide them with a baseline to prioritise strategic investments. It brings about an awareness beyond the Technology function into Risk, Business and the Boardroom, where informed discussions around insurance policy and risk hedging can be undertaken. It creates a level of awareness on cyber exposure across the organisation (for example, with the Legal and Communications teams) that is difficult to achieve otherwise, enabling preparedness in scenario response.

Despite the benefits, many organisations either often shy away or overlook the need to dive deeper into quantifying their cyber risk exposure. Understandably, quantifying cyber risk is not an easy task. With limited historical data available, it is challenging to put a number or sensible range to a scenario that is difficult to predict. It requires a familiarisation of the nature of attack as well as internal processes and infrastructure across the organisation. This presents a greater challenge in quantification as organisations typically lack a formally defined risk appetite that drives decisions around risk management. When there is limited understanding on how cyber risk should be managed, it also becomes increasingly challenging to estimate the cost related to specific investment or activity.

However, quantification is all about probability, not certainty. It is meant to provide a directional view around the level of risk an organisation should be prepared to manage rather than a definitive answer that provides an accurate measure. Given the evolving nature of threats and regulatory landscape, there is also a need to reassess the estimation regularly.[1]

Quantification of cyber risk would help organisations deep dive into understanding their exposure and provide them with a baseline to prioritise strategic investments.

1 Annual review of estimation is recommended to ensure that it is reflective and relevant. However, ad-hoc review is recommended if there are significant changes in regulations, processes or systems within the organisation.

Quantification can significantly change the dialogue and strategic application of cyber risk management, if used appropriately. Organisations are increasingly recognising the value of cyber quantification measurement. According to the Marsh Microsoft Global Cyber Risk Perception Survey 2019, which heard from more than 1,500 cross-industry respondents globally, the number of organisations, who undertake a quantitative cyber risk measurement method such as Value-at-Risk (VaR)[2] modelling, has almost doubled from 17 percent in 2017 but remains low, overall. With the new level of awareness and collaboration among various stakeholders, the quality of available data and sophistication of models will only improve over time to deliver more accurate and useful outcomes.

In the previously published *"Taming Cyber – Quantifying cyber risk using a structured scenario approach"* report, Oliver Wyman introduced the structured scenario approach to the cyber risk quantification process. Building on the framework, one may then ask how to conduct an effective quantification process. Specifically, how to translate a technical view on assets and their risk into a relatable concept that broader organisation stakeholders can relate to? How to ensure that quantified risk is relevant to organisations rather than an academic exercise? These questions can be addressed through careful and concrete use of scenarios, each with its specific narrative, loss drivers, and overall estimation.

BENEFITS

- Uncovers various implications (tangible and intangible) from a financial standpoint
- Clearer understanding of organisation's probable cyber exposure and its impact
- Enables informed discussion around transfer of risk through insurance
- Catalyst to increase awareness beyond IT to the rest of the organisation
- Informs educated investment in reducing overall cyber exposure

CHALLENGES

- Constantly changing landscape of attack as hackers become more advanced and unpredictable
- Organisations typically lack a formally defined risk appetite that drives business decision and strategy around risk management
- Limited historical data and scarcity of detailed publicly available information on cost of cyber attacks making it difficult to model cyber risk
- Cyber risk management not fully integrated into Enterprise Risk Management, increasing overall barrier and visibility to CXOs. Potential misplaced focus on prioritising protection of IT assets over business assets

2 Value-at-Risk (VaR) is a measure of potential risk. In the context of cyber risk, VaR indicates potential loss that could be incurred in the event of an actual cyber attack.

1 NARRATING realistic scenarios

Quantification becomes challenging in the absence of clarity. Therefore, the more specific we can be in the scenario narratives, the easier it is to guide the conversations on estimation. However, this is easier said than done since it is difficult to narrate an incident that has never realistically occurred before.

To manoeuvre this and develop compelling scenario narratives, below are the common pitfalls that should be avoided. Keeping these in mind, it would help provide the necessary clarity to narrate a scenario that clearly articulates the cause, event and impact towards the organisation's operations.

BOILING THE OCEAN WITH GRANULAR SCENARIOS
In case of uncertainty, there is a tendency to ensure coverage across as many potential scenarios as possible. Do not boil the ocean with many different scenarios without priorisation and alignment. Agree on the top 3-5 scenarios that align most with your assessment criteria and focus on those.

BASELINING AGAINST TOO MANY DATA POINTS
Similarly, once a scenario is selected, a common tendency is to narrate it across as many severity levels as possible to reflect all probabilities. This is challenging in many ways and the marginal benefit in doing so is minimal. Hence, narrating scenarios at 2 levels of severity: e.g. Material (1-in-2 years) and Extreme (1-in-30 years), is sufficient.

MISALIGNMENT OF NARRATIVE AND THE ORGANISATION'S RISK CONTROLS
Developing narratives without aligning to the organisation's existing control weaknesses and critical assets can lead to lengthy debate and a lack of trust in the quantification. Therefore, reflect your understanding of the organisation in your narratives.

FALLING INTO THE TRAP OF DATA AVAILABILITY/UNAVAILABILITY
In the absence of clarity, many institutions anchor against historical incidents. On the other hand, institutions may also dismiss certain important scenarios, due to the unavailability of data to support quantification. While important, there is a fine line between using historical data as a baseline and falling into its trap because over time security enhancements would have been introduced, processes might have been redesigned and external threat landscape could have changed, making historical data directionally relevant, at best.

ENABLING POTENTIAL BIASES TO INFLUENCE PERCEPTIONS
Stakeholders provide views that can be influenced by a set of biases: over-confidence, optimism, motivational bias, memory bias, structural bias, etc. All of these can potentially influence the quantification processes. Hence, being aware of them and taking mitigating actions would be important (e.g. benchmarking information, playing devil's advocate, and engaging relevant subject matter experts).

2 QUANTIFYING scenarios

Once a specific narrative is in place, relevant stakeholders from different teams and departments need to be engaged to help analyse the scenario response actions and the estimated cost drivers for both material and extreme attacks. Depending on the maturity of the organisation's risk appetite and scenario response management, this may require several iterations before arriving at an estimate.

To assist stakeholders from different business units to analyse the scenario response actions and estimated costs, we recommend using the following as a benchmark to kick-start discussions:

DATA FROM PREVIOUS SCENARIOS (CYBER OR NON-CYBER) WITHIN THE ORGANISATION

- **To extrapolate costs incurred** in marketing campaigns, hiring of legal counsel, system enhancements, public relations (PR), etc.
- **To identify scale and volume of impact** based on the number of impacted customers, number of vendors, number of transactions, backup restoration, service-level agreement (SLA), etc.

CYBER ATTACKS ON OTHER ORGANISATIONS

- **To determine a potential scenario response plan** in brand-building, system enhancement cost, PR and notification, etc.
- **To ensure estimates are reflective** of the current **external threat landscape**

While benchmark figures can be used to steer stakeholder conversations in the right direction, it is critical that these figures are not applied as-is. This is because some of the data may be masked by underlying lack of disclosures. Additionally, benchmarks from different organisations may not reflect the level of security controls, governance, and processes within a different organisation. An organisation's data from past scenarios, on the other hand, may no longer be reflective of its current risk profile due to changes in processes and enhancements in security over time. More importantly, organisations need to understand that they are up against cyber threats that are ever-evolving, and past benchmarks may or may not remain relevant against the latest threats. Hence, a level of assessment and an extrapolation of figures will be necessary.

The development of these narratives and estimates would require stakeholders to conceptualise the possibilities. Therefore, quantification is both an art and a science. Ensuring that stakeholders internalise and are comfortable with this concept would be the greatest success factor in quantifying cyber risk.

ILLUSTRATING A **MATERIAL SCENARIO**
Theft of customer data

When narrating a scenario of a material nature, keep in mind that this is the most severe event that an organisation has seen – perhaps an event that most can relate to and will commonly see in the news. Typically, they are more contained and have limited impact, which the organisation can easily recover from. Through initial scenario analysis and identification, imagine that data theft has been assessed as one of the top cyber exposure areas within your organisation. Let's walk through how one would navigate through the narratives and work towards quantification of the event with a material severity in mind:

SCENARIO NARRATIVE

"Alex, a privileged user within the organisation stored his administrative login details on an unsecured notepad online. As the head of the credit card team, Alex had access to the Personally Identifiable Information (PII) of millions of customers.

Their login details were leaked, enabling a hacker to access customer data from a local database that they had access to (one that is not protected by a security-enhanced centralised database). The hacker was able to steal sensitive data of over 1,000 customers (fortunately none that would enable fraudulent transactions) which was made available on the dark web. Early detection limited the scale of impact to the organisation."

SCENARIO ANALYSIS

We can break down the storyline into the following components:

- **Vulnerability "gap":** Alex, a staff with privileged access without appropriate controls and adequate cyber awareness
- **Actor:** Hacker with malicious intent
- **Asset:** Database containing sensitive customer data
- **Modus operandi:** Hacker used Alex's credentials (hence not blocked by database protection measures) and stole customer data
- **Impact:** Customer data made available on the dark web
- **Mitigation:** Early detection through 3rd party services scanning the dark web

ESTIMATION OF LOSSES

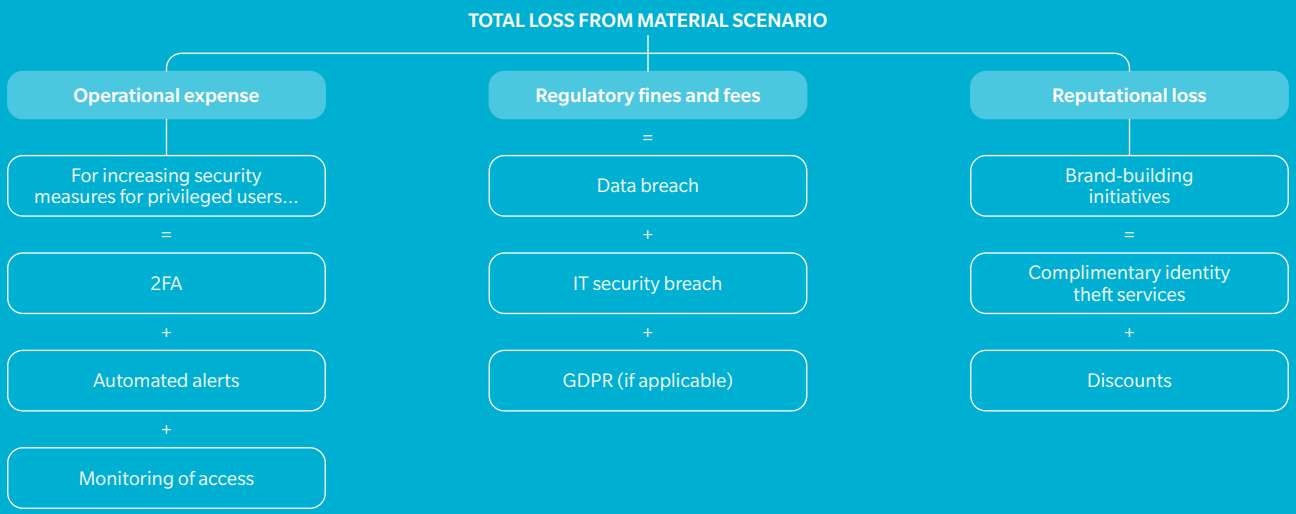
Based on the narrative, an estimation for data theft attack of material nature would require (but not limited to) stakeholders from the IT security teams, Legal, Compliance, impacted business unit, PR and Marketing teams to be involved in discussions.

To drive initial conversation between privileged users, historical data can be used as a baseline to estimate potential costs. Using cost to implement two-factor authentication (2FA) as an example, historical cost can be used as a baseline and existing infrastructure set-up can highlight the number of critical databases where 2FA needs to be implemented.

Hence, this can be logically derived as:

Cost of implementing 2FA = Number of critical databases x Cost of implementing 2FA per database

SCENARIO LOSS DRIVERS



ILLUSTRATING AN **EXTREME SCENARIO**
Compromise of SWIFT (Banking payments network) environment

When compared to a material scenario, an extreme scenario can be seen as a "black swan event" that an executive may only see once in a career. It typically comes with significant loss impact – involving customers, regulators and third parties – making it more difficult for the organisation to recover from such an event. To illustrate an extreme attack, let's look at the compromise of SWIFT environment – an information exchange system for financial transactions between institutions world-wide – as one of the top cyber exposure areas within a Financial Services (FS) organisation:

SCENARIO NARRATIVE

"A long delay in internal software patching left the organisation's infrastructure vulnerable to attack. A group of organised hackers gained access to the SWIFT environment through the vulnerability and planned a sophisticated attack, gaining access to different points of approvals. This enabled hackers to edit and create new SWIFT messages to process fraudulent transactions.

The hackers remained dormant for months leading up to the attack, but within a short 8-hour period they were able to transfer and cash out a substantial sum of money to different parts of the world."

SCENARIO ANALYSIS

We can break down the storyline into the following components

- **Vulnerability "gap":** Delay in internal software patch
- **Actor:** Hackers with malicious intents
- **Asset:** SWIFT network
- **Modus operandi:** Hackers use the vulnerability "gap" to perform fraudulent transactions on SWIFT
- **Impact:** Monetary loss for customers
- **Mitigation:** Internal alert on detection of large-value transactions

ESTIMATION OF LOSSES

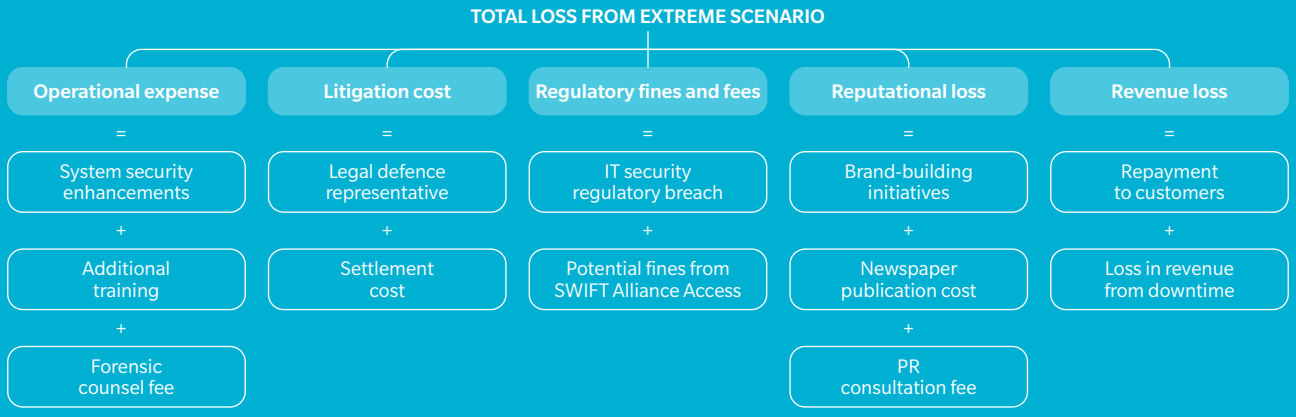
As compared to a material attack, the estimation for an extreme SWIFT attack would require a larger group of stakeholders. Extrapolation from external events and historical data will be useful to indicate potential initiatives, actions, and an estimated cost.

Consider the cost of repayment due to fraudulent SWIFT transactions, it is difficult to calculate the exact number of successful fraudulent transactions and the respective value of each case. An example of such an extreme event, the Bangladesh Bank SWIFT heist – a theft of $81 million through four transactions and another $20 million via a single transaction – informs us that SWIFT attacks are typically of large value and through a smaller number of transactions. Applying this to the organisation's internal SWIFT transaction data, extrapolation of the required figure can be estimated:

Cost of repayment from fraudulent SWIFT transactions = % of transactions impacted X Number of transactions per day X Average value of transactions per day

The more extreme the case, the more challenging it is to quantify the drivers. However, this is meant to provide a directional view instead of a definitive view for an informed decision-making.

SCENARIO LOSS DRIVERS



3 The so-what of modelling **CYBER EXPOSURE**

Individual scenarios give us the loss exposure for individual scenarios – which can be correlated to one another – arriving at a single Value-at-Risk (VaR) number. This single VaR number can be useful as a measure of probable cyber risk exposure for the organisation. However, the approach for deriving the VaR number is considered to be quite theoretical and there are several assumptions made to derive the final VaR number – making it much less tangible than loss exposure for individual scenarios. As a result, most organisations focus on quantification exercise for the benefit of understanding the exposure in specific cyber scenarios.

With the information of individual loss exposures in hand, the organisation can make an informed decision around the level of "protection" confidence that the organisation would desire and the resulting strategic risk decisions to help reduce exposure. Possible decision-making insights include:

STRATEGY FOR CYBER INSURANCE

Most organisations do not have a well-defined strategy for purchasing cyber risk insurance. Thus, they often over-pay for protection in areas where it is not required, and lack adequate coverage in required areas. The process of cyber risk quantification can help organisations identify the most significant areas of exposure and the amount of protection required to help define a thorough strategy for the protection. Moreover, demonstrating the understanding of cyber defences through a comprehensive quantification approach can also help get discounts from insurers!

PRIORITISATION OF CYBERSECURITY INVESTMENTS

Given cyber security is a fairly technical topic, prioritisation of security budget can be hard. Using the quantification approach, and estimating impact on loss exposures to drive prioritisation is a transparent way of prioritising budget for all stakeholders.

ONGOING MONITORING OF CYBER READINESS

Ultimately, loss exposure number is an indication of an organisation's status vis-à-vis ever-evolving cyber threats. As the organisation invests in building cyber resilience, potential exposure of the organisation to cyber risks should decrease, reducing the loss exposure number. Ongoing monitoring of the loss exposure number can give senior management and the Board insights into the cyber readiness of the organisation and help identify areas requiring further attention.

CONCLUSION

As high-profile cyber incidents impacting well-known names across different industries are increasingly making headlines, the perception that cyber risk is solely an IT-related issue no longer holds true. The question remains – will you leave your organisation's fate to the unknown? Or will you take charge to make sure that your organisation is not next to be featured on the front-page news?

Raising awareness and transparency across the organisation serves as the first step in mitigating cyber risk. By quantifying cyber risk, we open informed discussions throughout the organisation – on how and what the organisation can do to increase its cyber resilience and build capabilities. Ultimately, this will help the organisation realise that the fight to protect against cyber attacks is not an IT or Risk function responsibility, but one for the whole organisation.

AUTHORS

WOLFRAM HEDRICH

Executive Director, Marsh & McLennan Insights
wolfram.hedrich@oliverwyman.com

JAYANT RAMAN

Partner, Finance & Risk Practice, Oliver Wyman
jayant.raman@oliverwyman.com

TANISHQ GOYAL

Engagement Manager, Oliver Wyman
tanishq.goyal@oliverwyman.com

EVA WOON

Associate, Oliver Wyman
eva.woon@oliverwyman.com

RACHEL LAM

Research Analyst, Marsh & McLennan Insights
rachel.lam@oliverwyman.com

The authors would also like to thank Laura Novilia Gunarso for her contribution to the paper.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

ASIA PACIFIC
+65 6510 9700

EMEA
+44 20 7333 8333

AMERICAS
+1 212 541 8100

www.oliverwyman.com

ABOUT MARSH & McLENNAN INSIGHTS

Marsh & McLennan Insights uses the unique expertise of Marsh & McLennan Companies and its networks to identify breakthrough perspectives and solutions to society's most complex challenges.

Our work draws on the resources of Marsh, Guy Carpenter, Mercer and Oliver Wyman – and independent researchers. We collaborate with industry, government, non-governmental organisations, and academia around the world to explore new approaches to problems that require shared solutions across economies and organisations.

Marsh & McLennan Insights plays a critical role in delivering the MMC Advantage – Marsh & McLennan's unique approach to harnessing the collective strength of our businesses to help clients address their greatest risk, strategy and people challenges.

OLIVER WYMAN