CREST

CMAGE
Cyber Security Maturity Assessment Global Ecosystem

Good Practice Guide

How to Deliver Quantitative Analysis

January 2023

Regulators

How to Deliver a CMAGE - Quantitative

Contents

Executive Summary

- Quantitative Assessment of cyber risk is an increasingly prominent topic in cyber security
- The requirement for a quantitative approach to assessing cyber risk stems from the need to understand an accurate, consistent, up-to-date picture of risk relating to multiple entities. This need cannot be satisfied by simply scaling more traditional qualitative approaches
- Currently, Quantitative Assessments are most frequently used to manage third-party risk, guide cyber insurance offerings, manage a distributed portfolio of entities and drive cyber security standards
- Quantitative risk assessment involves collecting data and information from various sources and then applying a consistent methodology and a set of best-practice principles to process and generate ratings from the data.
- Leading providers of quantitative risk assessment can also use cyber threat intelligence to add threat context to vulnerability data and provide a more accurate overall picture of risk
- There are considerable opportunities to refine quantitative assessment models and better integrate them into business-as-usual cyber security practices.

Introduction

The Quantitative Assessment of cyber risk is an increasingly common and important discipline in cyber security. We define Quantitative Assessment as the: “Collection and analysis of a range of data sets to provide an understanding of cyber risk factors associated with an entity or group of entities.”

More and more people need to assess the cyber risk associated with companies accurately, quickly and at scale. Traditional approaches to risk assessment are not suitable for this.

So, here we set out a new methodology and explain what best practice looks like.

- Introduce the topic
- Explain why it has become so prevalent
- Contrast Quantitative Assessment of cyber risk with traditional, qualitative approaches
- Describe how Quantitative Assessment of cyber risk can be conducted
- Establish best practice principles
- Analyse why threat intelligence is so important for Quantitative Assessment

- Describe current use cases
- Identify some areas for maturation and development of the field.

About CREST

CREST is the international not-for-profit accreditation and certification body representing the technical information security industry.[1] CREST’s mission is to build high-quality capability, capacity and consistency within the global technical cyber security sector.

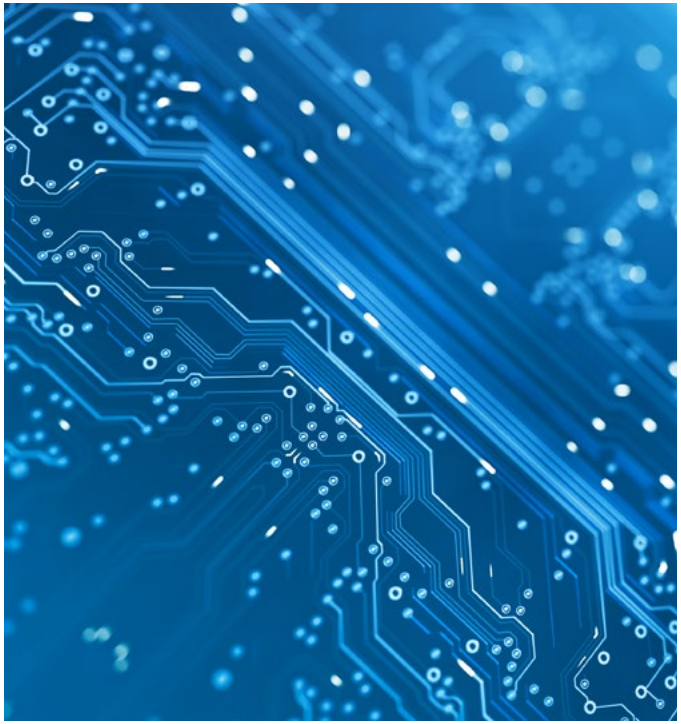
CREST focuses on professionalising the technical cyber security market while driving the quality and standards of organisations operating within it.

This helps mature countries’ domestic cyber security capability while allowing for international opportunities and consistency. It also provides greater assurance that the depth and breadth of skills in a country are aligned to the needs of the buying community.

CREST has developed this capability, capacity and consistency via whitepapers on cyber security issues and topics.

CREST commissioned this whitepaper to communicate to all stakeholders – including practitioners, customers, regulators and others – what best practice is in conducting a Quantitative Assessment of cyber risk at an individual company, sector and country level.

3 CREST



What is Quantitative Assessment of Cyber Risk? Why and how is it used?

1.0 What is Quantitative Assessment of Cyber Risk?

1.1 Definitions

For this white-paper, Quantitative Assessment is defined as collection and analysis of a range of data sets to better understand cyber risk factors associated with an entity or group of entities at any level.

Quantitative Assessment of cyber risk differs from the more traditional **qualitative approach**, which usually occurs through human-led information collection via interviews and subsequent analysis.

Risk is defined as a combination of threat, vulnerability and impact[2], as illustrated in Figure 1 (see below).

[2] *CREST*

Figure 1: Threat, Vulnerability and Impact illustration

1.1.1 How is Quantitative Assessment delivered?

Increasingly in the cyber security sector, various companies provide quantitative cyber risk assessment of via delivery of cyber risk rating scores.

This approach is similar to credit rating. Organisations of all types receive risk ratings based on automated collection and analysis of various cyber risk data sets.

However, the practice of Quantitative Assessment to deliver cyber risk ratings is still a nascent field.

Accordingly, there are many different approaches to collecting and analysing data to provide cyber risk scores.

This paper provides a background to cyber risk rating, focused on the following:

- What is the need for Quantitative Assessment of cyber risk?
- What are the primary use cases for Quantitative Assessment of cyber risk?
- What is best practice in the Quantitative Assessment of cyber risk?
- What next for Quantitative Assessment?

Cyber Risk Ratings

Figure 2: Typical Cyber Risk Ratings

1.0 What is Quantitative Assessment of Cyber Risk?

1.2 What is Driving the Need for Quantitative Assessment of Cyber Risk?

Scale

One of the key drivers in adopting quantitative approaches to risk management is the requirement to manage risk at scale. The typical qualitative approach tends to be both labour-intensive and specific to a single organisation, neither of which are particularly replicable. The requirement to assess risk at scale derives from more mature, forward-looking risk management programmes conducting assessments beyond the confines of their own organisation.

Standardisation

Although the core components of a qualitative approach to addressing risk (see methodology section) will likely remain constant from one engagement to another, the process features a litany of variables and subjective inputs that can create various results.

This subjectivity can make it difficult to accurately compare the level of risk assessed for different entities. This is not necessarily an issue for a standalone risk assessment of a single organisation. But an approach requiring ranking or comparison of different levels or categories of risk needs a consistent, standardised approach that can be rolled out across several subjects.

Speed

One of the key advantages of quantitative approaches to assessing cyber risk is how quickly new ratings can be generated. While a sophisticated baseline capability will take significant resources to establish and refine, once in place, providers can undertake large Quantitative Assessment projects with minimal effort, simply pulling records from their existing databases of assessed entities.

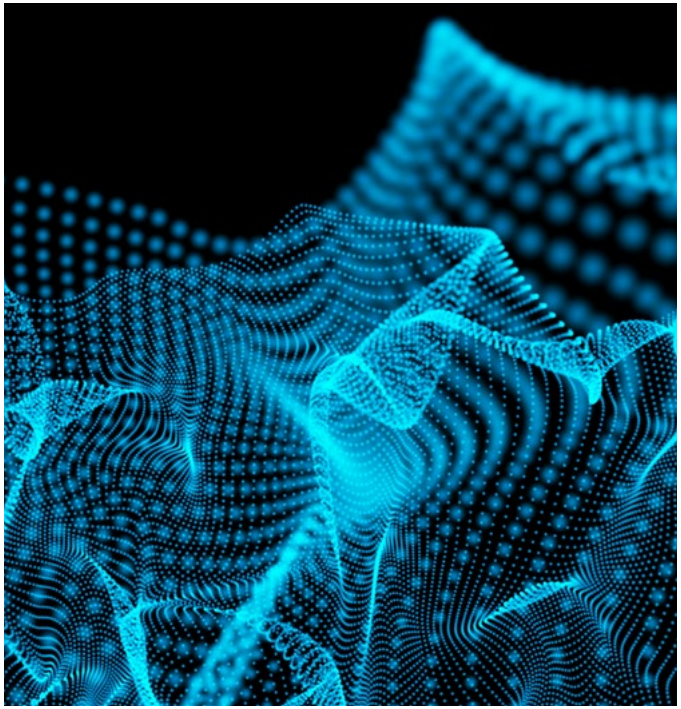
Recency

Related to the above point regarding speed, a quantitative approach to risk also allows you to quickly refresh and update your understanding of risk in response to changing circumstances. The cyber risk landscape means new data on threats and vulnerabilities are constantly becoming available, while the requirement to have this up-to-date picture is another factor driving its adoption.

Risk

Cyber security's gradual transformation from being considered a purely technical issue and an extension of IT to a critical strategic risk that requires appropriate board level attention, has also contributed to the growth in qualitative approaches to assessing risk.

As a result, risk-based approaches to cyber security (mirroring the approach to conventional security) have become more fundamental to securing an organisation and making it more resilient in response to cyber risks, largely at the expense of a more compliance-driven approach. It follows that companies are extending these efforts with more rigorous and Quantitative Assessments.



1.0 What is Quantitative Assessment of Cyber Risk?

1.3 What are the main use cases for Quantitative Assessment of Cyber Risk?

Managing third-party risk

Changes in the cyber threat landscape have also driven the requirement to adopt a quantitative approach to risk assessment.

For example, increasing integration of IT services between companies and the advent of supply chain compromises (where a threat actor looks to compromise a trusted partner to provide an easier route into the target organisation) as a tactic by sophisticated adversaries mean companies need to better understand the level and nature of risk associated with their third parties.

This can be used for both diagnostic – selecting between two potential third parties based on their contrasting level of risk – or remediation purposes, for example, to help address specific vulnerability or threat issues pertaining to third parties.

Cyber Insurance

The growth in the cyber insurance market is another key determinant in adopting quantitative approaches to risk assessment. The total value of gross written premiums will grow from US$2.5bn in 2015 to an estimated US$21bn in 2025.[3]

Though the growth of big-game hunting ransomware operations since 2019 has challenged the existing model, insurers have sought to develop more reliable, rigorous methods to accurately calculate risk associated with their insurance and price premiums accordingly. In turn, this is driving quantitative methods of assessing risk.

Acquisition

In keeping with the general increase in recognition of cyber risk as a critical issue for boards, the cyber security posture of a potential acquisition is an increasingly important consideration for the process. The £18.4m fine issued to Marriott in 2020 because of a 2014 breach affecting Starwood Hotels, which it acquired in 2016, indicates the type of potential risk acquires are assuming as part of this process.

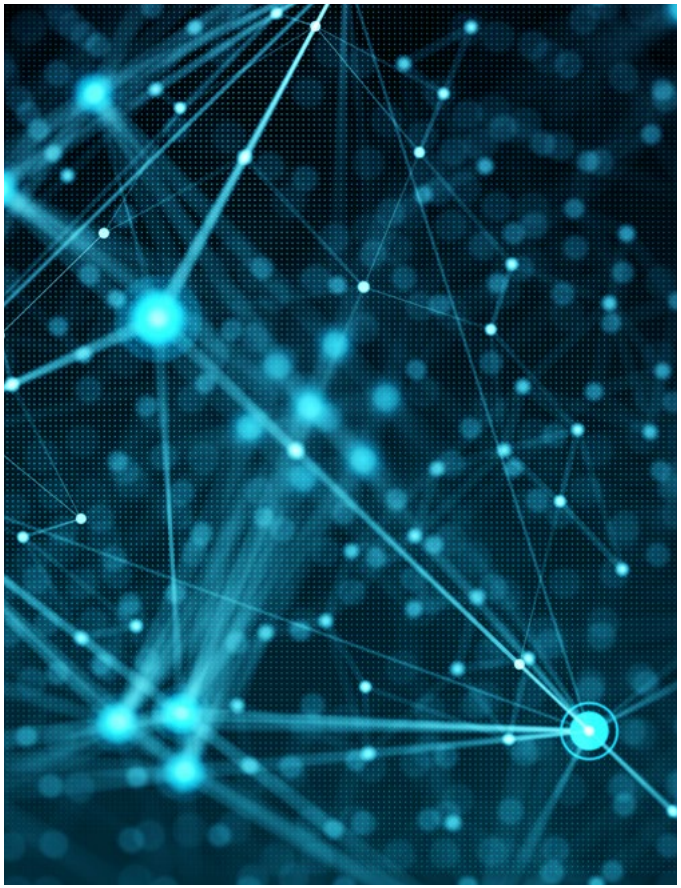
Quantitative Assessment of cyber risk is becoming an increasingly common element of mergers and acquisitions, both to inform the negotiation process, understand the maturity of the other party and prepare for post-deal integration.

Portfolio management

Multinational companies with geographically distributed business units have sought to use Quantitative Assessment common methodology to assess cyber risk associated with their disparate entities.

Similarly, holding companies with portfolios or organisations operating multiple brands with separate infrastructure have used Quantitative Assessment methodologies to provide standardised assessment of their assets.

[3] *Insurance Times*



1.0 What is Quantitative Assessment of Cyber Risk?

1.3 What are the main use cases for Quantitative Assessment of Cyber Risk?

Regulators

With cyber resilience of their regulated entities an increasing priority, forward-thinking regulators are increasingly using some method of Quantitative Assessment to collectively assess different levels of cyber risk among their regulated entities. This visibility allows them to evaluate the efficacy of current cyber risk reduction programmes, prioritise resources and drive remediation initiatives in response.

Board engagement

Despite the wealth of data with which they operate, Quantitative Assessment methods can reduce and simplify complex and abstract data sets into easily accessible metrics.

This has made them attractive to non-technical and executive audiences. This is especially true where quantitative rating providers can add context by tracking the change of risk ratings over time - showing return on investment – and add context by comparing the company to its competitors and benchmarks for its size, sector and country.

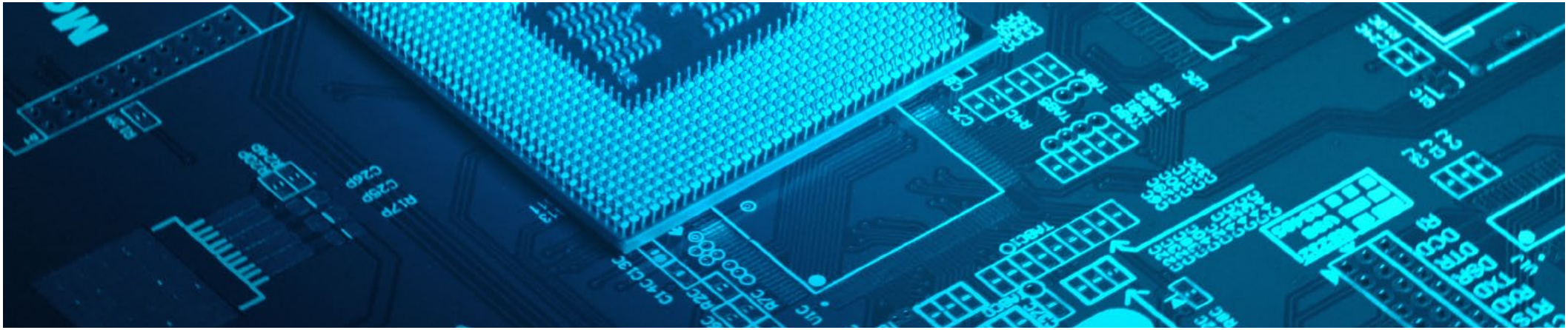
Forrester assesses that Quantitative Assessment ratings will become a de facto standard in boardrooms by 2025.[4]

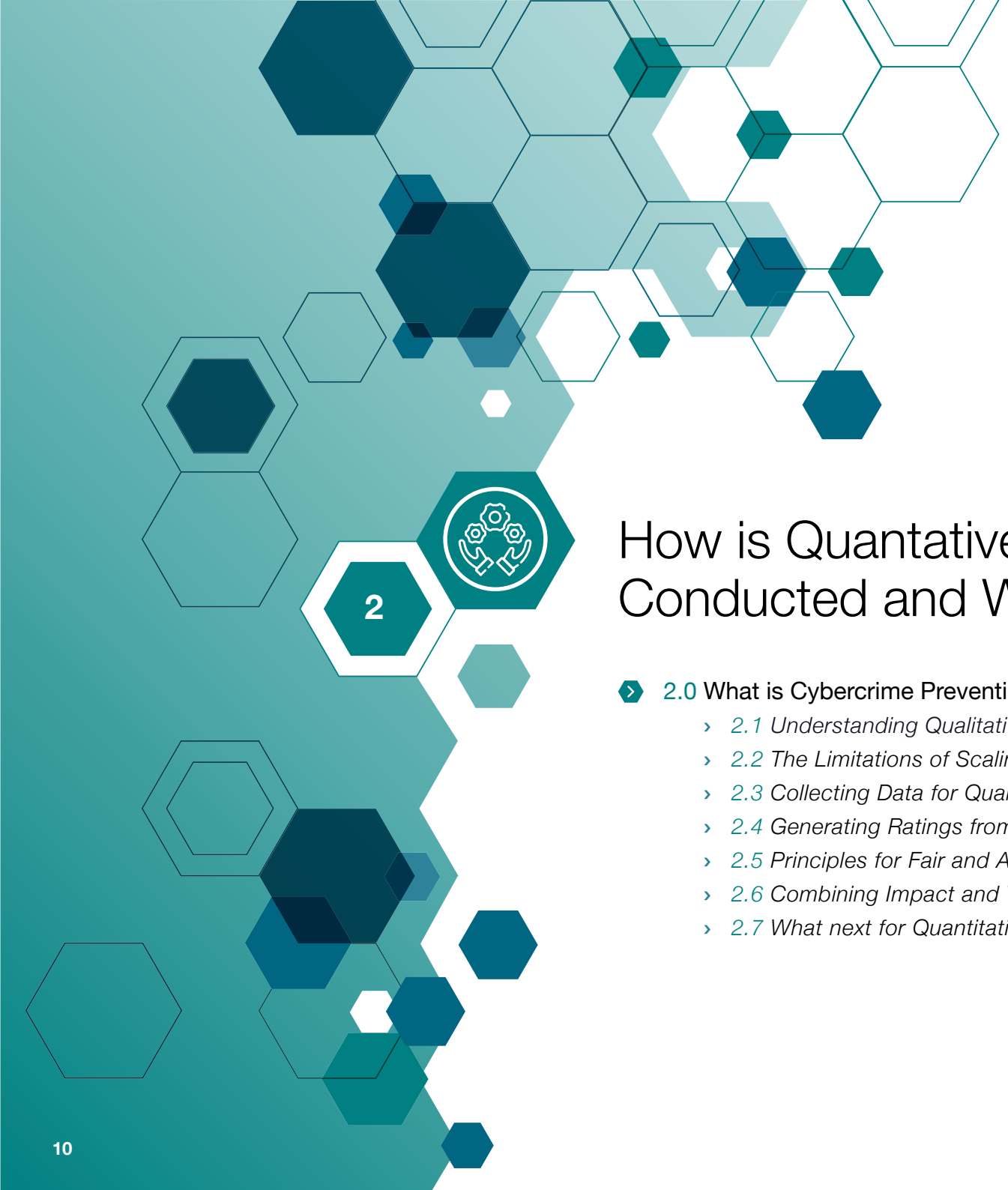
Driving standards: Understanding the cyber risk associated with different sectors and countries via a Quantitative Assessment process can also allow for the delivery of cyber security initiatives.

CREST has assessed overall levels of financial sector cyber security maturity in several developing countries, of which Quantitative Assessment of cyber risk represented a core component.

[4] *Forrester, 2020*

> *"Forrester assesses that Quantitative Assessment ratings will become a de facto standard in boardrooms by 2025."*





2

How is Quantative Assessment Conducted and What is Best Practice?

- 2.0 What is Cybercrime Prevention?
  - *2.1 Understanding Qualitative Approaches to Cyber Risk Assessment*
  - *2.2 The Limitations of Scaling this Approach for Quantitative Assessment*
  - *2.3 Collecting Data for Quantitative Risk Assessment*
  - *2.4 Generating Ratings from Data*
  - *2.5 Principles for Fair and Accurate Security Ratings*
  - *2.6 Combining Impact and Vulnerability Data with Threat Intelligence*
  - *2.7 What next for Quantitative Assessment?*

2.0 How is Quantitative Assessment conducted and what is best practice?

2.1 Understanding qualitative approaches to cyber risk assessment

The traditional approach to assessing cyber risk – and conventional security or other risk categories – has been more qualitative. A qualitative risk assessment can be completed using several methods, including the Delphi Technique, Bow Tie analysis, the Structured What-if Technique, and applying the Pareto Principle.[5]

However, the most common and accessible form of qualitative cyber risk analysis is via an impact-likelihood matrix. We describe this process here to better understand and contrast it with quantitative approaches to assessing risk.

This qualitative approach typically involves a process of information gathering from key organisation stakeholders, typically via questionnaires or interviews and occasionally supported using structured analytic techniques.

The process involves identifying a series of risk events split across multiple categories, typically including:

- **Operational** – an outage or disruption to production processes
- **Reputational** – adverse media coverage damages the standing of the organisation
- **Financial** – loss of revenue or operating profit
- **Legal** – potential prosecution or related issues
- **Regulatory** – the introduction of additional compliance requirements

The information gathering process typically entails high-level assessments of the relative likelihood of these events materialising and the assessed impact on the organisation if they do. High-level categories for each of these can help prioritise different risk events – for example, ranking likelihood from very low to very high and calculating dollar values associated with the different types of impact.

Although this process involves basic numerical elements, it remains a fundamentally qualitative process – i.e. based on an individual's judgements and descriptive in nature – and is far removed from the quantitative approaches to risk assessment that are the focus of this paper.

[5] *Safran*

2.0 How is Quantitative Assessment conducted and what is best practice?

2.1 Understanding qualitative approaches to cyber risk assessment

Qualitative risk management processes tend to focus on a combination of high-likelihood, low-impact risk events and those that are less likely, but capable of producing a much more substantive impact on the business.

At this point, the entity should be able to engage in one of four main paths to dealing with identified risks:

- **Mitigate** – Identify a remediation plan to reduce the likelihood or impact associated with the risk
- **Transfer** – Use a third-party, such as an insurer, to assume liability for that particular risk
- **Avoid** – Change strategy, so the risk is no longer applicable to the organisation
- **Accept** – Understand potential likelihood and impact but do not mitigate, transfer or avoid it

The origin of cybercrime prevention as part of a coordinated national strategy for combating online criminality arose from the United Kingdom's Serious Organised Crime Agency (SOCA).

A cybercrime prevention team, created in 2011, focused on degrading and disrupting online criminal marketplaces alongside raising the on- and offline profile of the "cyber police" through its interventions at all levels of cybercrime.

It primarily focused on high volume, cyber-enabled crime. Between 2012 and 2013, there was a transition from one national law enforcement entity, SOCA, to its new manifestation, the National Crime Agency (NCA).

Within the new National CyberCrime Unit (NCCU) investigation was re-aligned from 'cyber-enabled', traditional crimes enhanced by digital technology, to 'cyber-dependent' crimes; new crimes that need and use technology solely to cause harm to technology and those using it.

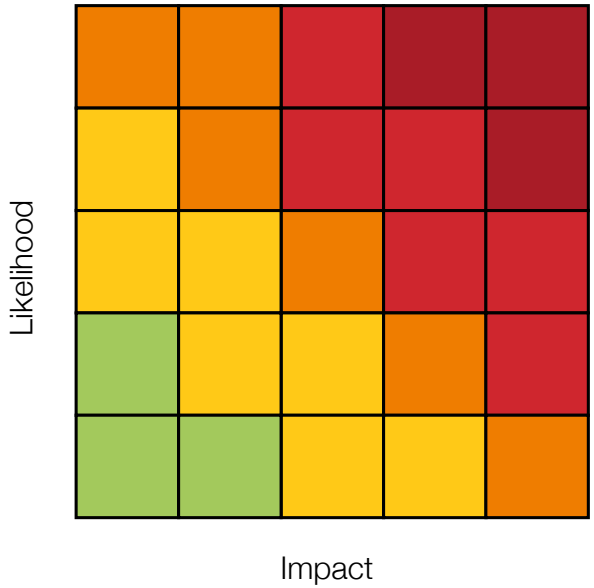


Figure 3: A typical likelihood-impact matrix used in qualitative risk assessments

2.0 How is Quantitative Assessment conducted and what is best practice?

2.2 The limitations of scaling this approach for Quantitative Assessment

Before the broader adoption of quantitative methods for assessing risk, companies used questionnaires to gauge risk level associated with third parties, most typically suppliers or vendors. This model – which sought to apply a qualitative approach at a broader scale – attracted these common criticisms:

Resource requirements

Questionnaires have proven challenging to issue, validate and administer within the organisation responsible for assessing risk.

Larger organisations with thousands of suppliers are more likely to have the dedicated resource to manage this requirement, though third-party risk assessment models dependent on this process can become unwieldy.

The need to complete a questionnaire as part of an on-boarding or procurement process also represents a cost (albeit much smaller) for subjects.

Questionnaire quality

Due to resource constraints, questionnaires will involve a trade-off between simplicity and accuracy. For example, questionnaires lend themselves to simple yes/no responses, though this model is less appropriate in risk assessment. A responder may state “Yes” to a question as to whether a specific control is in place, though this does not offer insight into its actual efficacy. Ascertaining this via questionnaire would require an approach more akin to a maturity assessment, imposing further resource requirements.

Subjectivity

Although the assessor can ensure consistency in the requirements of their questionnaire, the subjective nature of the format means responders will inevitably interpret and respond to questions differently.

As with the issue of questionnaire quality, efforts to standardise responses across entities will inevitably bring more resource requirements.

Self-attestation

Developing from the issue of subjectivity, the fact that questionnaires are self-assessed invariably means subjects are prone to exaggerating their strengths and downplaying their weaknesses to reduce the risk rating they generate - and entrench their relationship with the assessor. Validating these responses requires additional resources from the assessor, either adding to the labour-intensive nature of the process or requiring an approach other than questionnaires to provide guarantees.

Timeliness

Questionnaires represent a snapshot, or ‘point-in-time’ assessment of the risk associated with a responder. The responder’s business processes, technology stack, threat model, and a host of other factors will vary on continuously, rendering the responses in an annually refreshed questionnaire (for example) liable to be quickly out-of-date\ and inaccurate.

2.0 How is Quantitative Assessment conducted and what is best practice?

2.3 Collecting Data for Quantitative Risk Assessment

Quantitative risk assessment relies on collecting data from various externally accessible sources that can help provide insight into risk level associated with a particular entity. Individual sources and specific methodologies will vary between different providers of quantitative risk assessment. However, they generally include a combination of active (i.e., detectable) and passive techniques and integration of data from third-party sources and databases, such as internet registries.

The categories of data they collect typically include:[6]

- **Indicators of Compromise** – Any indication that the entity has suffered a historic breach or an ongoing attack
- **Attack surface** – Understanding potential vulnerabilities or misconfiguration on the entity's estate that may indicate a higher likelihood of compromise by adversaries
- **Service identification** – Assessing what technology is used by a particular entity
- **Domain name records** – Discovering endpoints where reachable services reside along with other configurations
- **Certificates** – Collecting certificates issued by authorities, self-signed and potentially expired certificates
- **Hosting arrangements** – Detecting shared hosting practices or use of content delivery networks
- **Security Infrastructure** – Identifying the use of web applications firewalls (WAFs) or other preventative measures
- **User information** – An indication that users are inadvertently leaking information or credentials that could potentially be weaponised against the entity
- **Company information** – Broader insight into the company, such as its sector and size

2.3.1 Intrusive vs Non-Intrusive Research

As quantitative risk assessment providers need timely and consistent access to data regarding the entities under assessment, they have developed a largely non-intrusive approach. This provides for scalability and timeliness of assessments and a methodology that can be applied consistently without engagement of assessed entities.

This non-intrusive approach carries limitations that providers have sought to address when they generate specific ratings from data (**addressed in the subsequent section**), and general principles (**see the section after next**) they abide by when administering Quantitative Risk Assessments for and on behalf of clients.

A more intrusive approach can help address any knowledge gaps or refine existing understanding, though in turn re-introduce the issues associated with qualitative approaches we addressed earlier.

[6] *Bitsight; RiskRecon; SecurityScorecard*

2.0 How is Quantitative Assessment conducted and what is best practice?

2.4 Generating Ratings from Data

Having collected this data, quantitative risk assessment providers then face the issue of collating the variety of inputs, accurately assigning them to different entities, and calculating a score or rating for each entity in question. This processing phase is unique to quantitative risk assessment, as qualitative processes will purely focus on the entity at hand.

Successful providers of quantitative risk assessment will typically engage in the following steps:

Demarcating between entities

Having collected significant volumes of data in the previous phase, accurate processing is required to assign it to different entities correctly.

Stale domain name system lookups, shared hosting, and content delivery networks can complicate attempts to attribute potentially vulnerable infrastructure correctly. QA providers need to ensure they have ways of tackling these issues.

Weighting of factors

Different categories of data collected have different implications for level of risk associated with a particular entity. For example, a high-profile company may attract significant chatter across social media or the deep and dark webs, though this could translate to a negligible threat against them. However, the presence of multiple critical-severity vulnerabilities on their estate is a better metric to measure their risk. An accurate risk assessment process should account for the disparity in value between these different indicators.

Asset function

Not all detectable assets are created equally. Certain assets carry a much greater organisational risk if they are misconfigured or vulnerable in a way that facilitates a compromise.

For example, vulnerable VPN instances or payment portals are much more likely to lead to a compromise if exploited than a WordPress plug-in. Therefore, they carry a higher level of risk. Understanding and accounting for these differences is crucial in accurate quantitative risk assessments.

Asset context

As well as the type of asset, context is critical in determining the level of risk associated with an individual asset. For example, risk associated with a misconfigured and accessible server in a test or staging environment will differ significantly from its counterpart in a production network. Where possible, quantitative risk assessment providers will account for the differing importance of such systems.

“Having collected this data, quantitative risk assessment providers then face the issue of collating the variety of inputs, accurately assigning them to different entities, and calculating a score or rating for each entity in question.

This processing phase is unique to Quantitative Risk Assessment, as qualitative processes will purely focus on the entity at hand.”

False positives

The passive and automated nature of data collection for quantitative risk assessment means providers may incorrectly designate infrastructure or assets as belonging to an entity other than its correct owner/operator.

This is especially important, considering the increasing awareness of attack surface management and the growing use of 'honeypots' and 'tar pits' on companies' estates, designed to distract and delay adversaries.

A more mature collection model - capable of verifying findings and attributing assets from a range of different sources - will reduce the rate of false positives.

However, providers should have mechanisms in place to facilitate these corrections, typically in an interactive manner via the platform on which they deliver their assessment.

Distributing scores

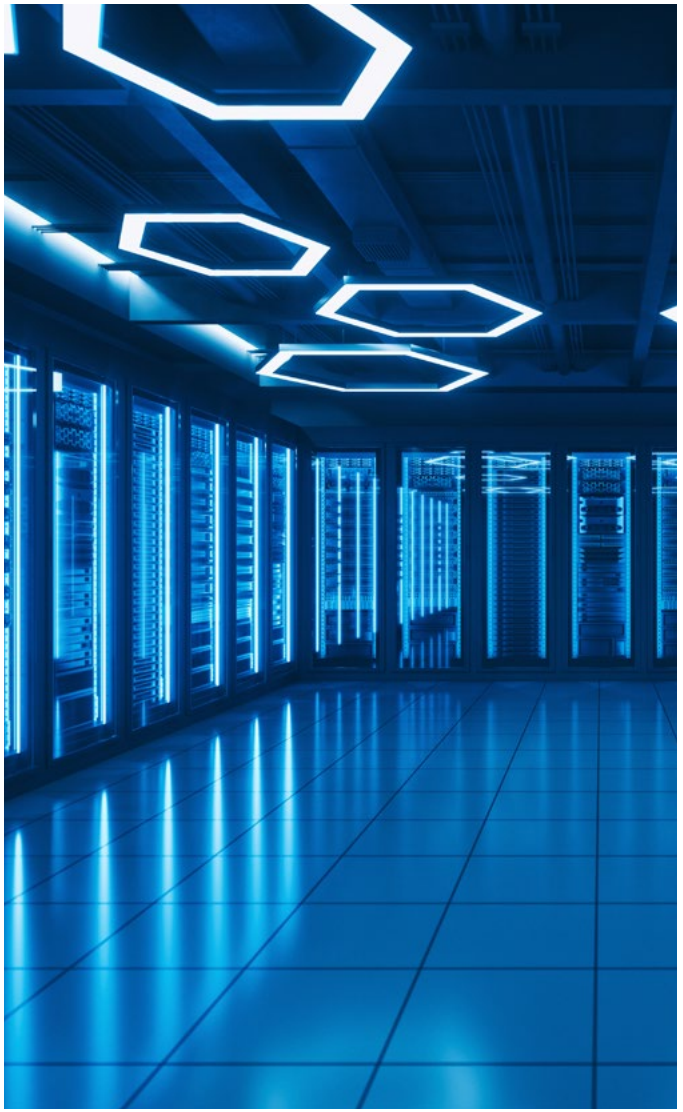
Quantitative Assessment scores are typically delivered as a numerical value (0-999), or a grade (A-F). Although these ratings and their definitions will naturally differ between providers, each provider must deliver consistent ratings with context.

Providers will typically look to establish a planned distribution of entities within their portfolio to explain what percentile the entities sit in, within the specific dataset for the Quantitative Assessment and how they relate to the average for their sector, country, and the entire dataset.

Accounting for actual breach data

Where possible, quantitative risk assessment models should be tested and have their methodology validated using data regarding actual breaches – for example, that held by insurers or publishers of mandatory disclosure information. The abstract nature of some data sources factored into any Quantitative Assessment model means corrections should be made where data is available.

"A more mature collection model - capable of verifying findings and attributing assets from a range of different sources - will reduce the rate of false positives."



2.0 How is Quantitative Assessment conducted and what is best practice?

2.5 Principles for Fair and Accurate Security Ratings

In June 2017, in response to the adoption of Quantitative Assessment methods for cyber risk, the US Chamber of Commerce issued a set of principles which providers should adhere to while using quantitative methods to analyse clients.[7]

The principles are:

- **Transparency** – Methodologies should be accessible to assessment subjects
- **Dispute, Correction and Appeal** – Subjects should be able to correct ratings by supplying data
- **Accuracy and Validation** – Assessors should validate their methodologies against available data
- **Model Governance** – Providers should share sufficient notice of changes to their model
- **Independence** – Commercial assessor-subject relationships should not affect ratings
- **Confidentiality** – Assessors should not share sensitive information on subjects with third parties

2.6 Combining Impact and Vulnerability Data with Threat Intelligence

As mentioned in the introduction, risk is a combination of vulnerability, impact, and threat. Most data types collected by quantitative risk assessors relate to the vulnerability element of risk, with fewer pertaining to impact. However, depending exclusively on these two categories of findings will restrict any attempts to properly quantify risk at scale, producing an incomplete and inaccurate picture.

Data sources regarding varying threat levels to the entity under assessment are a crucial determinant of the overall level of risk. For example, the nature and severity of the threat faced by a small online retail store in France will differ from those faced by a semiconductor manufacturer in Taiwan, even if they otherwise feature the same vulnerabilities or misconfiguration on their infrastructure.

Alternatively, as a portion of adversaries' targeting efforts are agnostic and dictated by technology, types of infrastructure, and hosting arrangements that companies use, providers can share insight into which technologies are more likely to be targeted by threat actors.

This is especially the case considering the current diffusion of proof-of-concept exploit code on the surface web, which offers a significant capability boost to threat actors that would otherwise lack the sophistication to exploit the vulnerabilities.

"Data sources regarding varying threat levels to the entity under assessment are a crucial determinant of the overall level of risk."

[7] *US Chamber of Commerce*

How is Quantitative Assessment conducted and what is best practice?

2.6 Combining Impact and Vulnerability Data with Threat Intelligence

Insight into how threats differ between entities can provide valuable context and qualifying information to the impact and vulnerability categories.

For example, two different organisations may feature the same number of similar-severity CVEs (**Common Vulnerabilities and Exposures**) on comparable assets on their infrastructure.

However, the threat posed to these specific vulnerabilities – as a result of proof-of-concept exploit code, evidence of intent to target the CVE or documented cases in which it has been exploited – could differ between the two entities, resulting in significantly different levels of risk.

The use of cyber threat intelligence in accurately delivering cyber risk ratings cannot be underestimated. Without including threat intelligence to complete the risk picture, cyber risk ratings providers are likely to be miscalculating risk scores. Given the increasing prevalence and importance of cyber risk rating, threat scoring is vital for any cyber risk rating approach.

Equally, the distinction between data and intelligence needs to be emphasised, as set out in CREST's Guide to "**What is Cyber Threat Intelligence and How is it Used?**"

"Instead of bombarding users with more data, CSR vendors need to focus on improving the risk context of their ratings to help security and risk pros prioritize efforts, support risk-based decisions, and act on the information."

2.0 How is Quantitative Assessment conducted and what is best practice?

2.7 What next for Quantitative Assessment?

The Quantitative Assessment field has made significant progress in recent years. Yet opportunities remain for further refinement and to add more value for its subjects.

The following list features some of the most critical areas in which practitioners can mature the field:

- Improvement: As articulated in the NCSC's supply chain cyber security principles, the core function of using quantitative risk assessment should be to drive continuous improvement
- Providers must focus on ensuring the action-ability of outputs of their Quantitative Assessment services, so risk can be reduced rather than just understood. Driving operational improvement is the "major market qualifier for CISOs",[8] which is likely to encourage a shift
- Enrichment: Quantitative analysis of cyber risk is currently restricted by its access to constantly available open-source data, which may not represent the entire picture of an entity's cyber risk
- There are opportunities for entities to enrich assessments and ratings by sharing additional data with providers regarding their security posture
- Although some subjects will understandably be reticent, this additional detail and transparency will enhance cyber security standards and decrease risk
- Regulation: Quantitative cyber risk assessment methods are likely to be adopted by regulators. They represent a vital element in a regulator's toolkit for understanding the contrasting maturity of their regulated entities - and allow for a more sophisticated risk-based approach to remediation rather than being restricted to compliance
- Reach: Current Quantitative Assessments focus on the infrastructure under evaluation. Quantitative Assessment methods will increasingly look to factor in the companies' products and services. This might include assessing APIs or providing validation for software updates to reduce the threat from supply chain compromises
- Refinement: Providers should use machine learning to refine their models and produce more accurate assessments. Improved datasets on incidents and losses from mandatory breach disclosure legislation and insurers will help refine and validate models

[8] *Forrester, 2020*

References

[1] Bitsight, “Cyber Security 101: Security Ratings Explained“, https://info.bitsight.com/cybersecurity-101-security-ratings-explained

[2] CREST, “What is Cyber Threat Intelligence and how is it used?”, https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[3] Forrester, “Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond”, https://www.forrester.com/report/Cybersecurity-Risk-Ratings-Market-Outlook-2020-And-Beyond/RES158178

[4] Forrester, “The Forrester New Wave: Cybersecurity Risk Ratings Platforms, Q1 2021”, https://www.forrester.com/report/The-Forrester-New-Wave-Cybersecurity-Risk-Ratings-Platforms-Q1-2021/RES161625

[5] Insurance Times, “Cyber insurance industry predicted to exceed $20bn GWP by 2025 – GlobalData”

[6] RiskRecon, “Introducing the updated RiskRecon Cybersecurity Risk Rating Model”, https://blog.riskrecon.com/a-new-approach-to-our-risk-ratings-model

[7] Safran, “An Introduction to Qualitative Risk Analysis”, https://www.safran.com/content/introduction-qualitative-risk-analysis

[8] Security Scorecard, “Explanation of our data“, https://securityscorecard.pathfactory.com/all/explanation-of-our-data

[9] US Chamber of Commerce, “Principles for Fair and Accurate Security Ratings”, https://www.uschamber.com/assets/archived/images/principles_for_fair_and_accurate_security_ratings.finallist_1.pdf

[10] Daniel Woods, Rainier Böhme, “Systematization of Knowledge: Quantifying Cyber Risk”, https://informationsecurity.uibk.ac.at/pdfs/WB2020_sok_cyberrisk_snp.pdf