Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment

James Crotty and Elizabeth Daniel
Faculty of Business and Law, The Open University, Milton Keynes, UK

Received 7 July 2022
Revised 8 September 2022
26 October 2022
Accepted 9 November 2022

Abstract

Purpose – Consumers increasingly rely on organisations for online services and data storage while these same institutions seek to digitise the information assets they hold to create economic value. Cybersecurity failures arising from malicious or accidental actions can lead to significant reputational and financial loss which organisations must guard against. Despite having some critical weaknesses, qualitative cybersecurity risk analysis is widely used in developing cybersecurity plans. This research explores these weaknesses, considers how quantitative methods might address the constraints and seeks the insights and recommendations of leading cybersecurity practitioners on the use of qualitative and quantitative cyber risk assessment methods.
Design/methodology/approach – The study is based upon a literature review and thematic analysis of in-depth qualitative interviews with 16 senior cybersecurity practitioners representing financial services and advisory companies from across the world.
Findings – While most organisations continue to rely on qualitative methods for cybersecurity risk assessment, some are also actively using quantitative approaches to enhance their cybersecurity planning efforts. The primary recommendation of this paper is that organisations should adopt both a qualitative and quantitative cyber risk assessment approach.
Originality/value – This work provides the first insight into how senior practitioners are using and combining qualitative and quantitative cybersecurity risk assessment, and highlights the need for in-depth comparisons of these two different approaches.

Keywords Cybersecurity, Risk assessment, Risk matrix, Quantitative, Qualitative, Bayesian statistics, Monte Carlo simulation

Paper type Full length article

Introduction

For most organisations, large or small and regardless of sector, the collection and storage of consumer, supplier and transaction digital data are of strategic importance [1]. This has resulted in many businesses storing large amounts of data, much of which is personally, commercially or financially sensitive. These data must be secured from malicious attack, loss or corruption to protect the on-going business, customer trust and corporate reputation and avoid regulatory redress [2].

The strategic reliance on digital data has resulted in cybersecurity being one of the most critical issues facing the leaders of organisations today. The cybersecurity approach adopted by many institutions is evolving from a methodology based on capability maturity to one that is risk based [3]. A qualitative approach to risk assessment utilising risk matrices is widely

Applied Computing and Informatics
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1108/ACI-07-2022-0178

employed in large part due to its promotion in standards and a perceived ease of use. However, the increase in computing processing power at a declining cost and the exponential growth in data held by organisations has prompted the emergence of a quantitative approach to cybersecurity risk assessment. This quantitative approach appears to address some of the known limitations of the qualitative method using risk matrices. However, it also presents its own challenges, including being considered more complicated to undertake and understand by users and decision makers that are not subject matter experts.

While qualitative cybersecurity risk assessment is widely used in practice [4, 5], there is little practical use of quantitative methods. In particular, there appears to be very limited studies comparing the practical use of qualitative and quantitative cybersecurity risk assessment approaches. The purpose of this research is to understand from practitioners how their organisations are navigating the use of qualitative and quantitative cybersecurity risk methods, and how both approaches might be adopted for more effective cyber risk assessment.

The study is based upon thematic analysis of in-depth qualitative interviews with 16 senior managers responsible for cybersecurity risk assessment. The originality of this work is that it provides the first insight into how senior practitioners are using and combining qualitative and quantitative cybersecurity risk approaches. The work is of value to cybersecurity practitioners and decision makers by demonstrating what others are doing, and is also of value to academics interested in impactful research as it demonstrates where practitioners would benefit from further research.

The following section reviews literature on the growth of corporate cybersecurity risk. Risk-based assessment is then introduced and both qualitative and quantitative approaches are discussed. The method adopted for this study is described and the findings of the interviews are presented. Conclusions, including opportunities for future work, are then provided.

Cyber threat: its origins and consequences

At the end of the last century digital assets accounted for just 25% of the world's data storage capacity. In sharp contrast, by the end of 2010 the share of data stored on digital assets had increased to over 90% – a proportion that continues to grow as data volumes expand at an exponential rate today [6–8]. Over the last decade there has been a major shift in where data are stored. In 2010, some 70% of the world's data were held by individuals on endpoint devices. Today, this estimate has halved to 35% with the majority of data now stored on enterprise assets [7]. This change is being fostered by enterprises utilising digitisation to remain competitive and seeing data as a source of value creation [9]. Knowingly or unknowingly, consumers are facilitating this effort too by their increasing use of online services and growing reliance on enterprise storage capacity. This trend is set to become significantly more pronounced with the realisation of the Internet of Things (IoT), resulting in an active installed IoT device base of some 31bn, generating data estimated to exceed 79ZB, by 2025 [10]. While these developments may provide significant new business opportunities for organisations, they also impose significant new responsibilities as firms increasingly become stewards of the world's data.

At the same time as global data volumes have been growing, cyber threats to these assets have become pervasive [11]. While cyber threat agents range from nation states to script kiddies, by far the most active are cybercriminals accounting for over 80% of cyber incidents [12]. Consequently, every organisation, from very large to very small, utilising any form of electronic data exchange or networked storage, is subject to cyber threat [13, 14].

Regulators and other government agencies have responded to this rapidly changing cyber threat landscape by becoming increasingly intrusive and punitive in their oversight. This is

evident from Regulation (EU) 2016/679 of the European Parliament and Council, otherwise known as the General Data Protection Regulation (GDPR), introduced in 2018. GDPR empowers regulators to impose fines of €20m or 4% of an organisation's global turnover, whichever is higher [15]. Enforcement action under GDPR is not limited to data theft or loss. It can arise because of any loss of data confidentiality, integrity or availability [16]. While big technology companies have received the largest fines to date, GDPR penal actions are not limited to this sector. Other examples of significant penalties include H&M €35m, British Airways €22m, Marriott €20.4m, Vodafone Italy €12.3m, Austrian Post €9m and CaixaBank €6m [17]. In addition to being obligated to pay any imposed fines, organisations suffering a cyber incident must also meet the costs of customer redress, business interruption, revenue loss, reputational damage and security remediation.

With cyber-attacks becoming increasingly pervasive and regulators more punitive, the loss ratio experienced by insurers on their cyber risk book is growing. In response to this trend, insurers are not just demanding higher premiums but doing so while offering the same or reduced cover. The Association of British Insurers (ABI) estimates year-on-year global price increases to June 2021 at 32% with some premiums increasing by as much as 75% [18, 19].

A risk-based approach to cyber security

Boehm *et al.* [3] propose that the cyber security approach adopted by many institutions is evolving from a methodology based on capability maturity to one that is risk based and seeks to reduce enterprise specific cyber risks.

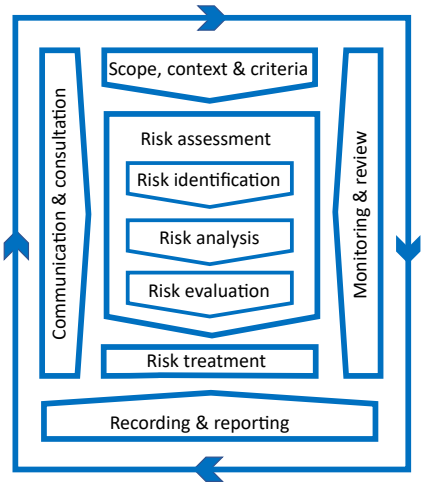
For a cybersecurity risk to exist an information asset must have a vulnerability that is exposed to a threat. A cyber risk analysis seeks to establish the likelihood of such vulnerabilities and threats occurring, and the resulting impact. Crotty and Daniel [20] recommend the implementation of a series of fundamental cyber risk controls applicable for all organisations and then, treating cyber risk as any other business risk, conduct an enterprise specific cyber risk assessment based on *ISO 31000:2018 – Risk Management* [21]. Such an assessment considers the nature of an organisation's assets, the threats and vulnerabilities these assets face, and the likely impact should these threats materialise. The process comprises risk identification, analysis and evaluation and the outcome is used to determine a bespoke risk management plan to avoid, reduce, transfer or retain risk according to the type and level of risk the enterprise can accept [21–23]. See Figure 1.

While a qualitative approach to cyber risk assessment is widely advocated and used, the effectiveness of these tools is challenged, and quantitative methods are proposed as an alternative or for augmentation.

Qualitative risk assessment

Multiple information security specific risk assessment tools have been developed based on *ISO 31000:2018*, which has become the de facto risk management standard [20, 24]. See Table 1.

The majority of the tools listed here utilise qualitative methods in the risk analysis phase of the process, adopting a two-dimensional risk assessment matrix where the axes are impact and likelihood, or variations of these descriptive labels. One or both matrix axes are ordinal scales, and the risk level or rating for each risk is calculated as the product of the likelihood and impact of each event [25]. See Figures 2 and 3. In contrast, while emphasising qualitative methods, both CIS RAM and MAGERIT refer to a quantitative approach to risk analysis using Bayesian statistics. The FAIR model alone is purely quantitative, based solely on Bayesian methods.



Source(s): Ref. [21]

Figure 1.
Risk management proces

Table 1.
Information security specific risk assessment tools based on *ISO 31000:2018*

CIS RAM	FAIR	ISF IRAM2
ISO 27005	ISMS	MAGERIT
NIST SP 800-30	Octave Allegro	OWASP

Source(s): Ref. [20]

Likelihood \ Impact	Insignificant	Minor	Moderate	Major	Catastrophic
Highly likely	High	High	Extreme	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Unlikely	Low	Low	Medium	High	Extreme
Highly unlikely	Low	Low	Medium	High	High

Source(s): Ref. [54]

Figure 2.
Risk matrix with "traffic light" and ordinal alpha rating scales

Likelihood \ Impact	Insignificant: 1	Minor: 2	Moderate: 3	Major: 4	Catastrophic: 5
Highly likely: 5	5	10	15	20	25
Likely: 4	4	8	12	16	20
Possible: 3	3	6	9	12	15
Unlikely: 2	2	4	6	8	10
Highly unlikely: 1	1	2	3	4	5

Source(s): Ref. [54]

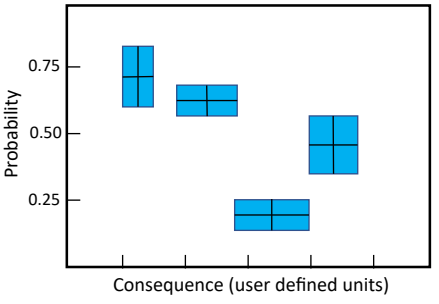
Figure 3.
Risk matrix with "traffic light" and ordinal numeric rating scales

BSI/IEC 31010:2010 [26] identifies 31 different risk assessment tools and techniques that it describes as qualitative, semi-quantitative or quantitative. Here, a risk assessment matrix is called a consequence/probability matrix and is said to be both qualitative and semi-quantitative depending on whether the matrix axes are ordinal alpha or ordinal numeric labels respectively.

The reasons cited for the use of qualitative methods for risk analysis include ease of understanding and implementation across all areas and levels of an organisation involved in ensuring cyber security, including the board and cybersecurity professionals. The absence of appropriate numerical data or resources to conduct a quantitative analysis is also mentioned [27, 28]. However, despite the widespread use of qualitative methods incorporating a risk matrix, the appropriateness of their usage is challenged. The basic premise that risk matrices are easy to use and understand is questioned, and it is proposed that the multiple factors determining the mapping of a risk event on such a matrix may not be well understood by users [4, 29, 30].

At a fundamental level, as the distance between the points on an ordinal scale is indeterminate, the practice of arithmetically combining numeric labels on ordinal scales to rank risks on a matrix has no mathematical logic [31]. Range compression, a key concern with risk matrices, arises from the grouping of risk ranges of likelihood and impact into discrete ordinal values on the matrix axes [29, 32]. Consequently, risks of a very different magnitude can be assigned the same rating. While a risk matrix seeks to cluster groups of equivalent risk in discrete groups of cells, there is no clear distinction in risk levels between adjacent cells of such a matrix or, indeed, within individual cells. Logical groupings of equivalent risk ratings cannot be found in a qualitative matrix and iso-risk lines on such a matrix are actually represented by hyperbola cutting across the boundaries of the matrix cells and different risk categories [5, 25, 33].

Various proposals to address the limitations of risk matrices have been made. Duijm [30] distinguishes between the use of risk matrices which, with limited risk levels, can be beneficial in deciding what risks to avoid or accept, but inadequate for the purpose of ranking of risks for mitigation. The use of log scales coupled with risk categorisation rules, incorporating risk ratings based on ordinal labels instead of colours or shades, is suggested to address range compression and constraints in equivalent risk grouping [34]. While this approach reduces the impact of the issues it seeks to address, risk differentiation is still dependant on the ranges used in the log scales of the matrix axes and risks of similar magnitude are not differentiated. A number of approaches based on probability consequences diagrams (PCDs) are considered, one being the mapping of each risk event as an uncertainty box on a continuous PCD rather than a discrete category on a risk matrix. Here, the centre of the box is the expected value of the event and the edges of the box a measure of uncertainty corresponding to prediction intervals [30, 35, 36]. See Figure 4.



Source(s): Refs [30, 35]

Figure 4.
Risk events mapped as uncertainty boxes on a continuous PCD

A further refinement to this is the overlay of a subjective strength of evidence and deviation risk for each risk event mapping [35]. This is intended to address the uncertainty inherent in the information used in a risk analysis even where objective probabilities are used. Providing a measure of this uncertainty is particularly important when there is separation between assessors and decision makers. Flage *et al.* [37] propose a certainty rating and reporting scheme where certainty is measured on a weak, medium, strong scale. Certainty is considered weak if just one of a number of criteria is not met including data being unavailable or not reliable, and a lack of agreement between subject matter experts. Set against these criteria, given the absence of a reliable body of frequentist data, the dependence on subjective views and the constantly changing cyber threat landscape, the level of certainty in cyber risk assessment must generally be considered weak.

While addressing some of the inherent weaknesses in risk matrices, an added difficulty with a continuous PCD is the need for a homogenous measure of consequence applicable to all risk events [30].

In addition to these structural challenges with risk matrices, other major concerns are cited: the need for risk matrix designers and users to fully understand the inherent weaknesses in them, the bias of users in making a qualitative assessment of risk, the inconsistent interpretation of labels by users, and only rarely is consideration given to risk correlations which could have significant impact on a risk assessment. The apparent simplicity of the use of risk matrices discourages necessary debate and the perceived precision of the rigour of analysis can lead to an unwarranted sense of confidence in the output on which risk mitigation plans will be decided [38]. For all these reasons, many advocates of quantitative risk assessment methods oppose the use of qualitative methods as unsound.

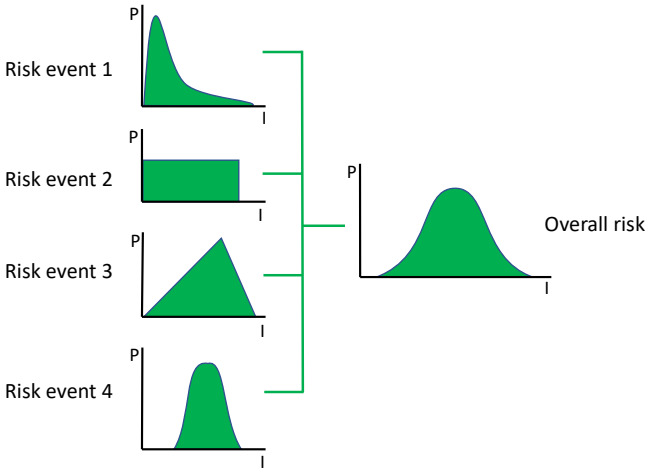
Quantitative risk assessment as an alternative

Viewed from an epistemology perspective, today's cyber risk assessment frameworks and models are predominantly based on subjective expert opinion rather than objective data [39]. While subjective knowledge is clearly relevant for qualitative risk assessment, it also has relevance for quantitative approaches.

Regarding cyber risk in particular, the availability of statistically analytical data to underpin objective knowledge is very limited for several reasons. There is inconsistency in the approaches of nation states and their agencies in gathering cyber security data and, in many instances, cyberattacks are unreported [39]. Given the rapidly changing nature of cyberattacks, relevant empirical data may not exist at the time of analysis. These constraints and concerns are amplified when considering the IoT where the number of IoT devices connected in a cyber–physical system may be unknown and the extent of the attack surface of such as system is significantly underestimated [40]. It is proposed that AI/ML and cognitive computing can help to address these challenges [40, 41], but it is also noted that such efforts could be undermined by bad actors gaining access to, and corrupting, the AI/ML training data and algorithms [39].

An alternative proposal to the ubiquitous use of qualitative matrices in risk assessment is the application of Bayesian methods to identify probability distributions for individual risks and employing Monte Carlo simulation (MCS) to determine a combined distribution for all these risk events. See Figure 5.

This approach, which can be used with only limited data, is facilitated by the selection of probability distributions for individual cyber risk events based on available data and subjective judgement [42]. The use of MCS has historically been constrained by the significant computer processing power it requires but this limitation has been alleviated in recent years by the now ready availability of extensive computing capacity at reduced costs. Despite the widespread use of this quantitative risk assessment approach in other disciplines



Source(s): Refs [32, 46]

Figure 5.
Aggregation of risk event probability and impact using Bayesian statistics and MCS

including engineering, finance, project management and software development [43–46] its employment in managing cybersecurity remains very limited. However, there is some advocacy for its use in this discipline also. Fagade *et al.* [47] explore how a quantitative approach enhances cybersecurity resource allocation while others contend that the qualitative methods so widely used today do not work and need to be replaced with a quantitative approach based on Bayesian statistics and MCS [32].

Quantitative methods address a number of the issues inherent in qualitative analysis. However, when only limited data are available these methods also require the subjective view of subject matter experts [48]. Of necessity, any bias in the input will be reflected in the output regardless of the method used [49, 50]. The probability theory employed in quantitative methods overcomes the fundamental flaw of subjecting ordinal scales to mathematical operations in qualitative tools, but this more rigorous mathematical approach may lead to an unwarranted sense of confidence in the results – one of the same concerns raised regarding results from qualitative analysis. Also, while the theory underpinning quantitative methods is long established, understanding and practical application of this theory may be challenging for many organisations.

The cyber security practitioners' view

Methodology

To obtain a cybersecurity practitioner perspective on the relative merits of qualitative and quantitative risk assessment methods, 16 industry practitioners from financial services and financial advisory services were interviewed using a structured interview guide. The finance sector was selected as it is a major target for cyberattacks and subject to extensive regulatory oversight, and hence requires the highest standards and expertise in cybersecurity practices. Interview topics included: their role, the organisation's approach to cybersecurity including standards and frameworks used, the benefits and challenges to this approach and how it could be improved with particular discussion of quantitative and qualitative methods and expectations for future approaches to cybersecurity. While the majority of the practitioner interviewees were CISOs or CROs, the views of ISMs, a CIO, EA and global cybersecurity implementation advisors were also sought in order to gather a range of informed insight.

Interviews were undertaken via online video conferencing and lasted between 1 and 2 hours and, with permission, were recorded to aid analysis. Thematic analysis was undertaken, commencing with repeated listening to the recordings and transcription of key parts. Initial themes were the topics from the interview guide and noted previously. These were inductively divided into 1st level sub-themes arising from the repeated study of the interviews, which were further subdivided into 2nd level sub-themes where helpful [51]. 1st level sub-themes included: concerns with qualitative approaches, lack of expertise and data for quantitative approaches, a need to combine both approaches and the role of cyber insurance. The 2nd level sub-themes included: "sea of green", speed of change, lack of data and rise in insurance premiums. Table 2 provides summary characteristics of the interviewees and interviews.

Findings

All of the respondents urged caution in not relying on either qualitative or quantitative methods alone.

Regarding qualitative methods, the interviewees referred to the false science of risk matrices which can result in a "sea of green" that does not reflect the reality of multiple

Role	Tenure	Sector	Employees	Remit	Geographic reach of organisation	Duration of interview
CISO[a]	4 yrs	Reinsurance	15 k	Group	Global	1 h
CISO	7 yrs	Payments	64 k	Group	Global	1 h
CISO	3 yrs	General Insurance	11 k	Group	Two + countries	1 h
CISO	3 yrs	General Insurance	6 k	Division[h]	Single country	2h
ISM[b]	5 yrs	Pension Mgt.	3 k	Group	Two + countries	1.25 h
ISM	3 yrs	Pension Mgt.	3 k	Group	Two + countries	1 h
ISM	2 yrs	General Insurance	400	Division	Pan-European	1.5 h
CRO[c]	6 yrs	Asset Management	2 k	Group	Single country	1.25 h
CRO	5 yrs	Pension Mgt.	3 k	Group	Two + countries	1.25 h
CRO	2 yrs	General Insurance	11 k	Group	Two + countries	1.5 h
CRO	3 yrs	Payments	500	Division	Pan-European	1.25 h
CRO	6 yrs	General Insurance	400	Division	Pan-European	0.45 h
CIO[d]	2 yrs	Payments	500	Division	Pan-European	1 h
EA[e]	3 yrs	Pension Mgt.	3 k	Group	Two + countries	1.5 h
GIA PH[f]	6 yrs	Financial Services	24 k	Group	Global	1 h
GIA TE[g]	3 yrs	Financial Services	24 k	Group	Global	1 h

Note(s): On Table 2
[a]CISO: Chief Information Security Officer
[b]ISM: Information Security Manager
[c]CRO: Chief Risk Officer
[d]CIO: Chief Information Security Officer
[e]EA: Enterprise Architect
[f]GIA PH: Global Implementation Advisor Practice Head
[g]GIA TE: Global Implementation Advisor Technical Expert
[h]All divisions are part of global organisations
Source(s): Ref. [20]

Table 2.
Profile of cybersecurity professionals interviewed

exceptions to policy creating unseen risk. The qualitative method used by all of the practitioners' organisations is a risk matrix. Though aware of the limitations of this approach and recognising that its apparent rigour may lead to unwarranted confidence in such an assessment, there is little emphasis placed on familiarising business decision makers with these constraints. However, quantitative methods are not seen as a panacea for the weaknesses of risk matrices.

Data on cyber risk events are limited and the speed at which the risk landscape is changing – including the highly dynamic nature of cyberattack methods and exponential increases in regulatory fines – makes a priori knowledge difficult to establish. They also expressed concern that quantitative methods can lead to a lot of analysis but not a lot of thinking and blindly following the actions dictated by the output rather than correctly challenging its validity.

Some of the companies of the practitioners interviewed already use a quantitative approach to determine cyber risk capital allocations and others are investing heavily in developing data driven approaches. But even these organisations still see a place for qualitative methods. The expectation is that the use of quantitative methods for cyber risk capital allocation will become pervasive over time as the volume and availability of cyber risk data increases. However, it is also expected that this emerging capability will be used in conjunction with current widely used qualitative methods rather than as an alternative.

Regarding cyber risk insurance, the interviewees noted that the terms imposed by insurance companies are becoming more onerous as cyber risk losses increase and, consequently, organisations adopting quantitative methods to help manage their cyber risk exposure may be viewed more favourably in the insurance underwriting process. They also thought that companies utilising all the tools at their disposal to manage cyber risk may be viewed more favourably by regulators in the event of a cyber incident.

Conclusions

As cyberattacks become ever more pervasive, regulators are becoming increasingly punitive in their response to incidents and cyber risk insurers are becoming more onerous in their pricing and terms for large companies and SMEs alike. Set against this context, it is recommended here that every organisation should have a cyber risk assessment and mitigation plan reflecting the nature of its assets, the threats and vulnerabilities these assets face and the likely impact should these threats materialise.

NIST [28] advocates the use of qualitative risk assessment methods to help ensure clear understanding and communication between decision makers and those providing expert opinion in a risk analysis. NCSC [23] reiterates this need for clarity but also recognises the advantages of using both quantitative and qualitative approaches. Similarly, an epistemological evaluation of risk assessment methods proposes that assessments based on both approaches are most reliable and, where available, the use of quantitative data is recommended to support subjective views [30, 39].

Our interviews with industry experts have shown that in practice cyber risk assessment approaches are predominately qualitative, despite widespread recognition of the limitations of these approaches. In some cases, detailed quantitative methods are employed to augment an initial qualitative assessment [45, 46, 52]. Even in cases where data are very limited, which is frequently the position in cyber risk assessment, the quantitative approach utilising subjective probabilities as proposed in this paper can be adopted.

The nature of risk assessment in general, and cyber risk assessment in particular, is such that pure quantitative analysis based on objective analysis of statistical data is not feasible. Consequently, the use of triangulation, which seeks more than one perspective from which to assess the cyber risk facing an organisation, can help provide a better understanding of the uncertainties involved and is recommended here [53]. While resource constraints may

prevent many organisations from using the quantitative methods discussed, the use of risk matrices and PCDs have merit, despite their recognised limitations and the latter not being used by the practitioners interviewed.

In the first instance, any organisation, large or small, can use a risk matrix to assess what risks to accept, avoid or accept subject to mitigation [30]. Working with this subset of risks to accept subject to mitigation, it may be more feasible to establish a measure of consequence for use in mapping this smaller range of risk events using uncertainty boxes on a continuous PCD for prioritisation. As well as potentially facilitating prioritisation, this process could help users to understand that risk matrices are not as simple to use as they appear, encourage meaningful discussion regarding the risks an organisation is facing and prompt the use of whatever quantitative data may be available. For organisations with the necessary resource, the quantitative approach described, based on Bayesian methods and MCS, should be employed for further triangulation.

Before any of the tools are deployed, it is important that practitioners and decision makers have an insight into the subjective nature of risk assessment based on the cited references and discussion here.

Government agencies and institutions such as the Association of British Insurers are seeking to gather data on cyber incidents and their associated costs [18]. As this body of information builds it offers the opportunity to reduce the subjectivity of a priori data currently used in risk assessment. How this impacts the effectiveness of quantitative methods and increase in their use, subject to the caveat that such data may become the target of bad actors, warrants study over time. More immediately, how the use of both qualitative and quantitative approaches by organisations might influence regulators in their assessment of cyber incidents, or the pricing and terms offered by insurance companies to underwrite cyber risk, should be examined.

References

1. Medeiros MMD, Maçada ACG. Competitive advantage of data-driven analytical capabilities: the role of big data visualization and of organizational agility. Management Decision. 2022; 60(4): 953-975.
2. Wang J, Wang L. The role of corporate reputation and crisis response strategies in data breach management. Journal of Management Information Systems. 2018; 35(2): 683-714.
3. Boehm J, Curcio N, Merrath P, Shenton L, Stähle T. The risk-based approach to cybersecurity. New York, NY: McKinsey & Company; 2019.
4. Ball DJ, Watt J. Further thoughts on the utility of risk matrices. Risk Anal. 2013; 33(11): 2068-2078.
5. Bao C, Dengsheng W, Jie W, Jianping L. Comparison of different methods to design risk matrices from the perspective of applicability. Proced Comput Sci. 2017; 122: 455-462.
6. Hilbert M, López P. The world's technological capacity to store, communicate and compute information. Science. 2011; 332(6025): 60-65.
7. Reinsel D, Ganz J, Ryding J. The digitization of the world from core to edge. Framingham, MA: International Data Corporation; 2018.
8. Roser M, Ritchie H. Technological progress. OurWorldInData.org; 2020.
9. Hippold S. Build a data-driven organisation. Stamford, CT: Gartner; 2018.
10. Vailshery LS. Internet of Things (IoT) – statistics & facts. Hamburg: Statista; 2022.
11. ENISA. ENISA threat landscape 2021. Athens: European Union Agency for Cybersecurity; 2021.
12. Verizon 2022 data breach investigations report. Basking Ridge, NJ: Verizon Communications; 2022.
13. SonicWall cyber threat report. San Jose, CA: SonicWall; 2021.
14. Symantec ISTR internet security threat report; 2019.

15. Council of the European Union European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Publications Office of the EU; 2016.
16. ICO. Guide to the privacy and electronic communications regulations. Cheshire: ICO; 2018.
17. Tessian. 30 biggest GDPR fines so far (2020, 2021, 2022). 2022.
18. Fraser L. Cyber insurance – growing the market to meet the global threat. London: Association of British Insurers; 2022.
19. Johansmeyer T. The cyber insurance market needs more money. Harv Business Rev. 2022.
20. Crotty J, Daniel L. Lessons from practice: insights on cybersecurity strategy for business leaders, from SMEs to global enterprises. Milton Keynes: Open University; 2021.
21. ISO Standard No. 31000:2018: Risk management. Guidelines (2018). Geneva: International Organisation for Standardisation Technical Committee; 2018.
22. Lam J. Implementing enterprise risk management from methods to applications. Hoboken, NJ: Wiley & Sons; 2017.
23. NCSC. The fundamentals of risk. London: National Cybersecurity Centre; 2018.
24. Bradley P. Risk management standards and the active management of malicious intent in artificial superintelligence. AI & Society. Springer; 2019.
25. Altenbach TJ. A comparison of risk assessment techniques from qualitative to quantitative. Oak Ridge, TN: Office of Scientific and Technical Information, US Department of Energy; 1995.
26. BSI. BS EN 31010:2010 Risk management. Risk assessment techniques. London: British Standards Institute; 2010.
27. BSI. BS 7799-3:2017: information security management systems. Guidelines for information security risk management. London: British Standards Institute; 2017.
28. NIST. NIST Special publication 800-30 risk management guide for information technology systems. Gaithersburg, MD: NIST; 2012.
29. Cox LA. What's wrong with risk matrices? Risk Analysis. 2008; 28(2): 497-512.
30. Duijm NJ. Recommendations on the use and design of risk matrices. Safety Science. 2015; 76: 21-31.
31. Hubbard D, Evans D. Problems with scoring methods and ordinal scales in risk assessment. IBM J Res Dev. 2010; 54(3): 2:1-2:10.
32. Hubbard DW, Seiersen R. How to measure anything in cybersecurity risk. Hoboken, NJ: Wiley and Sons; 2016.
33. Buck J. Risk matrices – why they don't work. Tann: B Advisory; n.d.
34. Levine ES. Improving risk matrices: the advantages of logarithmically scaled axes. J Risk Res. 2012; 15(2): 209-222.
35. Goerlandt F, Reniers G. On the assessment of uncertainty in risk diagrams. Saf Sci. 2016; 84: 67-77.
36. Ale B, Burnap P, Slater D. On the origins of PCDS – (Probability consequence diagrams). Saf Sci. 2015; 72: 229-239.
37. Flage R, Aven T, Zio E, Baraldi P. Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. Risk Anal. 2014; 34(7): 1196-1207.
38. Krisper M. Problems with risk matrices using ordinal scales. Graz: Institute of Technical Informatics, Graz University of Technology; 2021.
39. Radanliev P, De Roure D, Burnap P, Santos O. Epistemological equation for analysing uncontrollable states in complex systems: quantifying cyber risks from the Internet of Things. Rev Socionetwork Strateg. 2021; 15(2): 381-411.

40. Radanliev P, De Roure D, Page P, Van Kleek M, Santos O, Maddox LT, Burnap P, Anthi E, Maple C. Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars. Saf Extreme Environments. 2021; 2: 219-230.
41. Radanliev P, De Roure D, Walton R, Van Kleek M, Montalvo RM, Maddox LT, Santos O, Burnap P, Anthi E. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Appl Sci. 2020; 2(11): 1-8.
42. IBM. Monte Carlo simulation. Armonk, NY: IBM Cloud Education; 2020.
43. Yano M, Penn JD, Konidaris G, Patera AT. Math, numerics & programming (for Mechanical Engineers). Cambridge, MA: MIT; 2012.
44. Kroese DP, Brereton T, Taimre T, Botev ZI. Why the Monte Carlo method is so important today. Wiley interdisciplinary reviews. Computational Statistics. 2014; 6(6): 386-392.
45. Pergler M., Rasmussen A. Making better decisions about the risks of capital projects. New York, NY: McKinsey on Finance, McKinsey & Company; 2014.
46. Thelin S. Forecaster's toolbox: how to perform Monte Carlo simulations; 2018.
47. Fagade T, Maraslis K, Tryfonas T. Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. Int J Crit Infrastructures. 2017; 13(2-3): 152-167.
48. Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis; 1981. 1. 11-27.
49. Sharot T. The optimism bias. Current Biology. 2011; 21(23): R941-R945.
50. Dhami MK, Mandel DR, Mellers BA, Tetlock PE. Improving intelligence analysis with decision science. Perspectives on psychological science. 6th ed. SAGE Publications; 2015. 10. 753-757.
51. Bryman A. Social research methods. Oxford: Oxford University Press; 2015.
52. Safran. An Introduction to qualitative risk analysis. Stavanger: Safran; 2021.
53. Salkind NJ. Encyclopaedia of research design. Newbury Park, CA: SAGE Publications; 2010.
54. SAA. AS/NZS 4360:1999: risk management. Sydney: Standards Association of Australia; 1999.

Corresponding author
James Crotty can be contacted at: james_crotty@msn.com