KPMG

Cyber risk modelling and quantification

Rethinking cyber attack likelihood quantification

kpmg.co.uk/cyber

Contents

Summary

Let's face it: current approaches to modelling and quantifying cyber risk can be confusing. They often do not help decision-makers understand the true level of cyber risk exposure. They do little to help management understand which controls contribute more than others to reducing certain cyber risk exposures. They struggle to help management ensure they are focusing their resources on the areas of biggest 'bang-for-buck'.

Perhaps not surprisingly, management are often sceptical about the value that cyber risk modelling and quantification can deliver. They recognise it can help them make more informed decisions; they just aren't sure the benefit always outweighs the effort.

KPMG partnered with a large global insurance firm to address these issues. We developed an approach that would improve the firm's ability to de-construct and understand its cyber risks, optimise its cyber portfolio, and demonstrate robust decision making rationale in its governance structure.

In this paper, we share a snapshot of the results of our work.

We firmly believe that collaboration is key to managing exposures to the global cyber threat. And, just as attackers share information with each other, defenders must too.

We encourage you to participate in the development of this approach and to share your ideas, feedback and comments on the concepts outlined in this paper.

David Ferbrache
Global Head of Cyber Futures, KPMG

James Hanbury
Senior Manager, KPMG

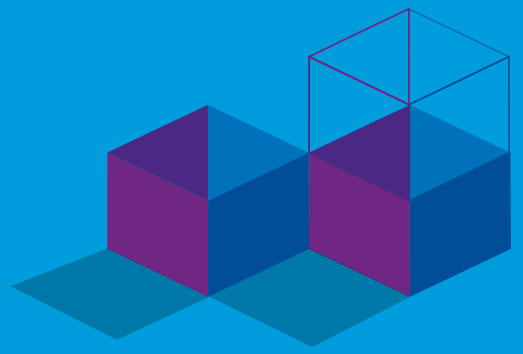
In this paper, we will show how cyber risk modelling and quantification can:

1. **Focus investment** on what matters for cyber risk reduction
2. Provide **robust** and **consistent decision making rationale**
3. Realise **business benefits proportionate to the implementation effort** involved

Challenge Modelling a 'complex problem'

Cyber risk is a complex problem – it has innumerable causes; it is tough to describe; and there is often not one single right answer. But that does not mean that it can't be modelled and managed.

We recognised there must be a better way to model and quantify cyber risk. We wanted to be able to de-construct the problem as best we could. We wanted to understand what cyber risks the organisation was exposed to and to what extent. And we wanted to find out what actions were contributing the most to reducing those risks.



"We wanted to know what actions would deliver the greatest cyber risk reduction for our customers and our lines of business. But the current models couldn't always tell us that. We needed to develop an approach that would provide our global cyber security team with a tool to support strategic cyber risk management and decision making."

Global CISO
Global Insurance Firm

"We set out to create a truly threat-led approach to understanding the firm's cyber risk exposure. It was about modelling the threat and understanding the layers of defence. It was about modelling attacker attack vectors and assessing their 'contact rate'. Perhaps most importantly, it was about converting the output into useful information for senior management that was grounded in good practice statistical methods."

Konrads Klints
Director, KPMG

Challenge What's wrong with the status quo?

In today's complex cyber risk environment, resilient organisations must be capable of:

- Efficiently and effectively reducing the likelihood of a successful cyber attack
- Quickly responding to contain and eliminate threats
- Rapidly recovering to minimise the impact on customers and business operations

> "We recognised we would never be able to definitively predict the likelihood or impact of a cyber attack. But we did know we could use our existing knowledge of our estate in better and more robust ways for cyber risk management. Our work with KPMG has helped close those gaps."

Global Head of Cyber Delivery
Global Insurance Firm

Traditional approaches to cyber risk management often involve a long list of so-called 'risks', RAG ratings and actions. For example, the 'risk' may be something like, 'exploitation of vulnerable systems' rated red because there's a big backlog of unpatched vulnerabilities.

These types of approaches have not typically considered:

- What the information means in the context of the true cyber risks we are concerned about (such as Ransomware, Data Breach or Business E-mail Compromise)
- How controls work together or compensate for another's failing
- Which controls really do contribute most to risk reduction
- How quantitative approaches can be used to properly answer these questions and reduce the potential for misguided management decisions which leave holes in cyber defences or makes poor use of security budgets

With growing investment in cyber security, Boards and Executives are looking more and more to see evidence of demonstrable risk reduction.

It is now more important than ever that investment decisions prioritise those controls which deliver the biggest bang for buck.

The Model Setting the model's principles

Our work was guided by five key principles across three phases:

Business alignment and expression of cyber risk

1 Speak the language of the organisation

Alignment: The risk model must align with current organisational risk frameworks and policies.

2 Consistency in the definition of a 'cyber risk'

Definition: Risks must be consistently defined as scenarios resulting in specific loss events.

Uplift quantification capability

3 Take a threat-led approach to modelling cyber risk scenarios

Focus: Scenarios must be modelled using a threat-led approach.

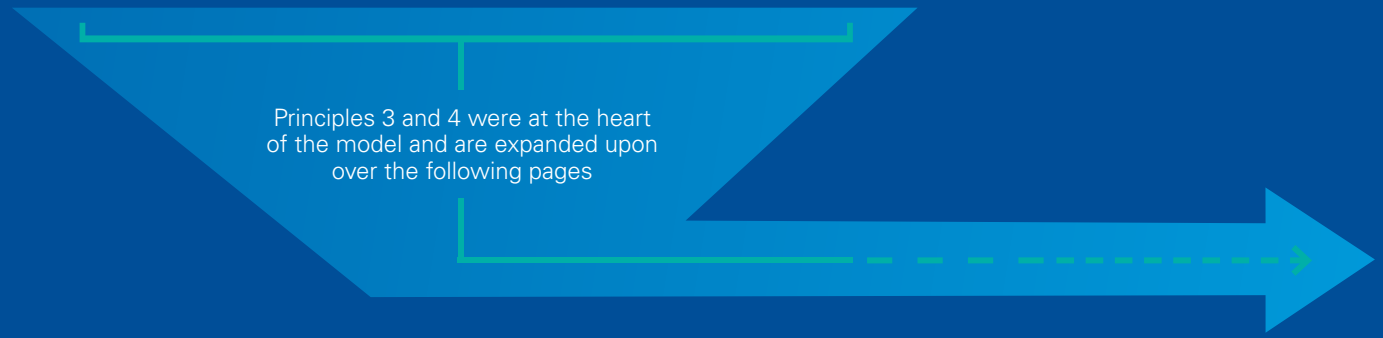
4 Use real-world data in calculations

Data: Likelihood and impact calculations must use real-world, internal and external empirical data.

Manage stakeholders

5 Understand the benefits and limitations

Understanding: The benefits and limitations of the model must be well communicated and understood.



The Model Three key inputs

1 Control classification

Classification of controls into three categories to simplify how we think about controls and how cyber risk is mitigated.

Likelihood controls:

Those controls which reduce the likelihood of a given cyber risk scenario materialising

Examples
Patch management
Anti-virus protection
DNS traffic scrubbing
Configuration management
Etc.

Impact controls:

Those controls which reduce the impact should the worst happen and a cyber risk scenario materialise

Examples
Crisis management
Backups
Forensic investigations
Cyber insurance
Etc.

Foundational controls:

Those controls that support the effectiveness of other controls

Examples
Asset management
Security architecture
Information security policy
Information classification
Etc.

2 Control effectiveness % estimations

We designed a framework to consider control effectiveness. For each control, we made quantitative % effectiveness estimations across three components.

The model supported both an automated and manual method of estimation. The automated method used the structured data available in the firm's GRC tooling, and the manual method allowed the CISO function to make more refined estimations.

There is opportunity in the future to use continuous control monitoring capabilities to further automate these estimations.

1) **Technical effectiveness:** How well does the control actually do the job it was designed to do?

2) **Process maturity:** How effective are the processes that enable, maintain and improve the control in doing what it was designed to do?

3) **Coverage:** To what extent is the control deployed across the risk-based portion of the estate it was originally intended for?

The Model Three key inputs

3 Scenario threat models

Modelling cyber risk scenarios to:

1) Capture the end-to-end process a threat actor must take to achieve their specific objective(s). This includes modelling the techniques a threat actor would use and therefore the organisational defences they need to defeat.

2) Capture the Boolean nature of how controls work. Does a threat actor need to defeat all controls or just the weakest control to achieve a given technique?

Key:

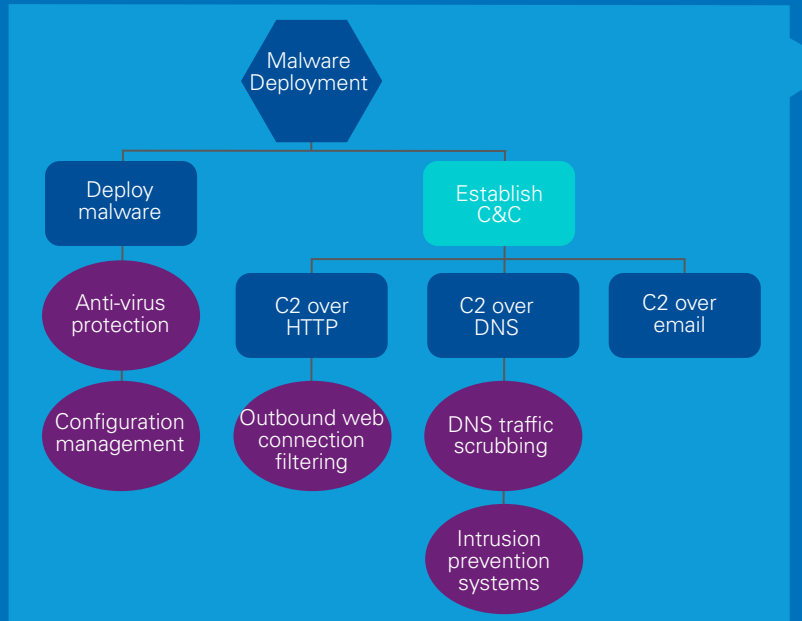
Threat modelling components

- Scenario
- Attack path step
- Technique
- Defence

Boolean operators

AND: Dependents of an AND node must all be achieved (i.e. all techniques) or defeated (i.e. all defences) and therefore a PRODUCT function is used for dependent % values.

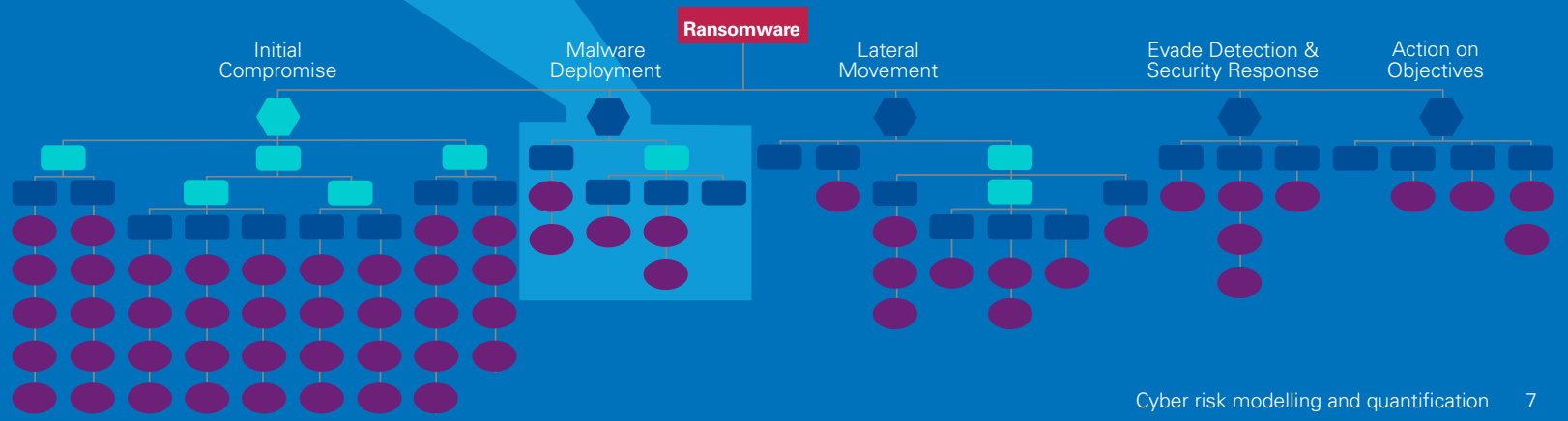
OR: Only one dependent of an OR node must be achieved (i.e. the most likely technique) or defeated (i.e. the weakest defence) and therefore a MIN/MAX function is used for dependent & values.



We used the well established attack tree concept to model a number of attack scenarios. We then built an automated method of converting these graphical models into tabular form in order to input into the calculation logic.

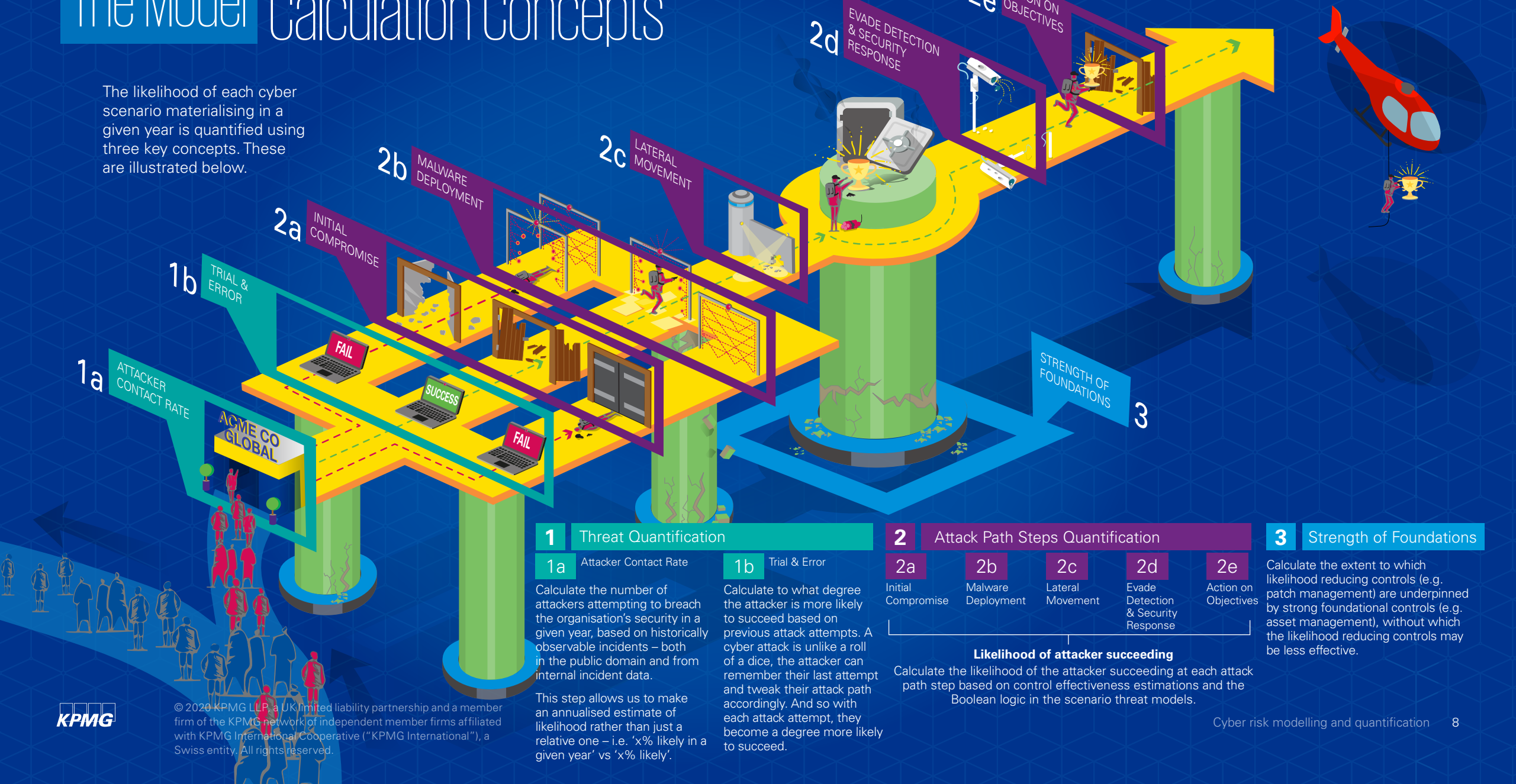
Example extract of model in tabular form

Node	Operation for Dependents	Precedent
Ransomware	PRODUCT	N/A
Malware Deployment	PRODUCT	Ransomware
Deploy malware	PRODUCT	Malware Deployment
Establish C&C	MAX	Malware Deployment
C2 over HTTP	PRODUCT	Establish C&C
C2 over email	PRODUCT	Establish C&C
Anti-virus detection	N/A	Deploy malware
Configuration management	N/A	Deploy malware
Outbound web connection filtering	N/A	C2 over HTTP
DNS traffic scrubbing	N/A	C2 over DNS
Intrusion prevention systems	N/A	C2 over DNS



The Model Calculation Concepts

The likelihood of each cyber scenario materialising in a given year is quantified using three key concepts. These are illustrated below.



1 Threat Quantification

1a Attacker Contact Rate

Calculate the number of attackers attempting to breach the organisation's security in a given year, based on historically observable incidents – both in the public domain and from internal incident data.

This step allows us to make an annualised estimate of likelihood rather than just a relative one – i.e. 'x% likely in a given year' vs 'x% likely'.

1b Trial & Error

Calculate to what degree the attacker is more likely to succeed based on previous attack attempts. A cyber attack is unlike a roll of a dice, the attacker can remember their last attempt and tweak their attack path accordingly. And so with each attack attempt, they become a degree more likely to succeed.

2 Attack Path Steps Quantification

2a Initial Compromise

2b Malware Deployment

2c Lateral Movement

2d Evade Detection & Security Response

2e Action on Objectives

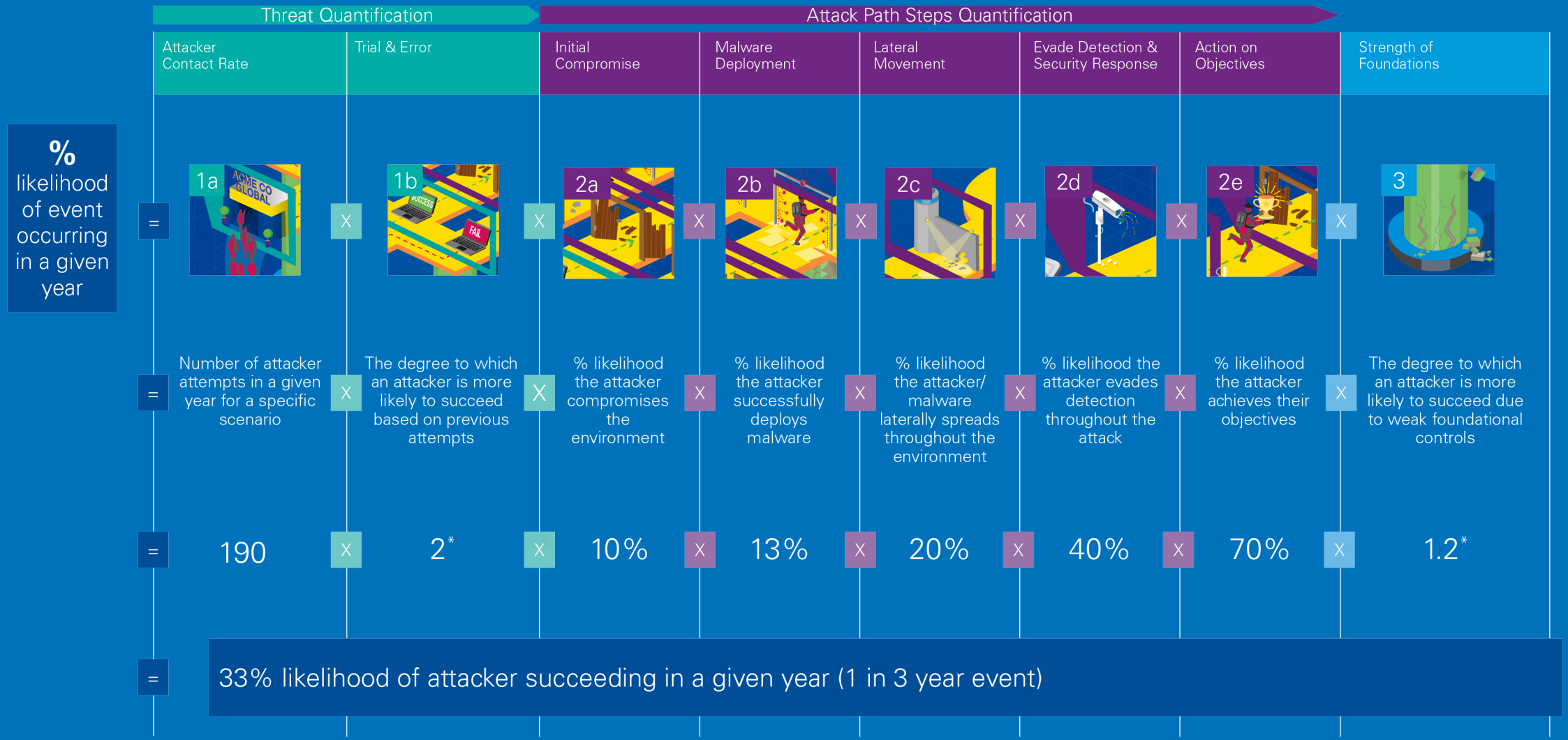
Likelihood of attacker succeeding

Calculate the likelihood of the attacker succeeding at each attack path step based on control effectiveness estimations and the Boolean logic in the scenario threat models.

3 Strength of Foundations

Calculate the extent to which likelihood reducing controls (e.g. patch management) are underpinned by strong foundational controls (e.g. asset management), without which the likelihood reducing controls may be less effective.

The Model Worked example

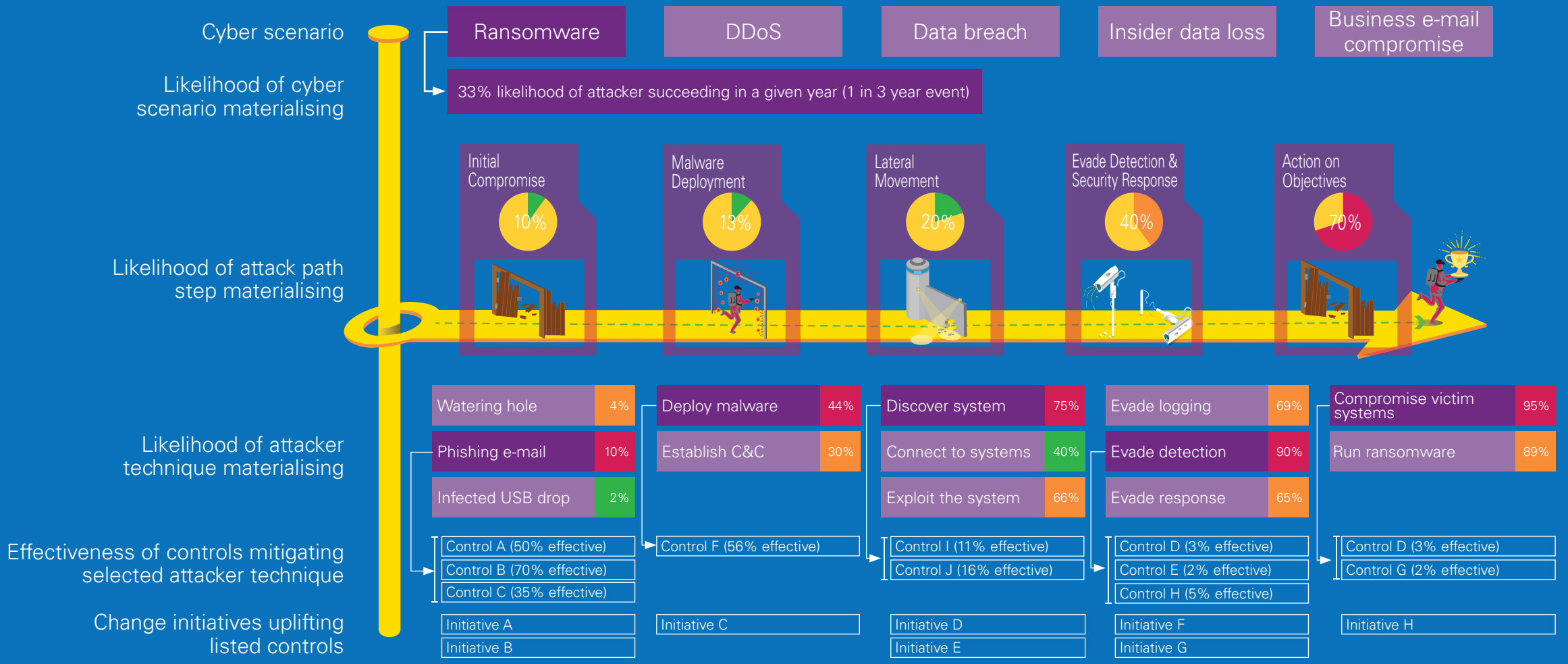


*The methodology for estimating these values is based on initial modelling, which we would love for, in particular, the community to help us refine.

The Model

Example outputs

Attack path weak spots



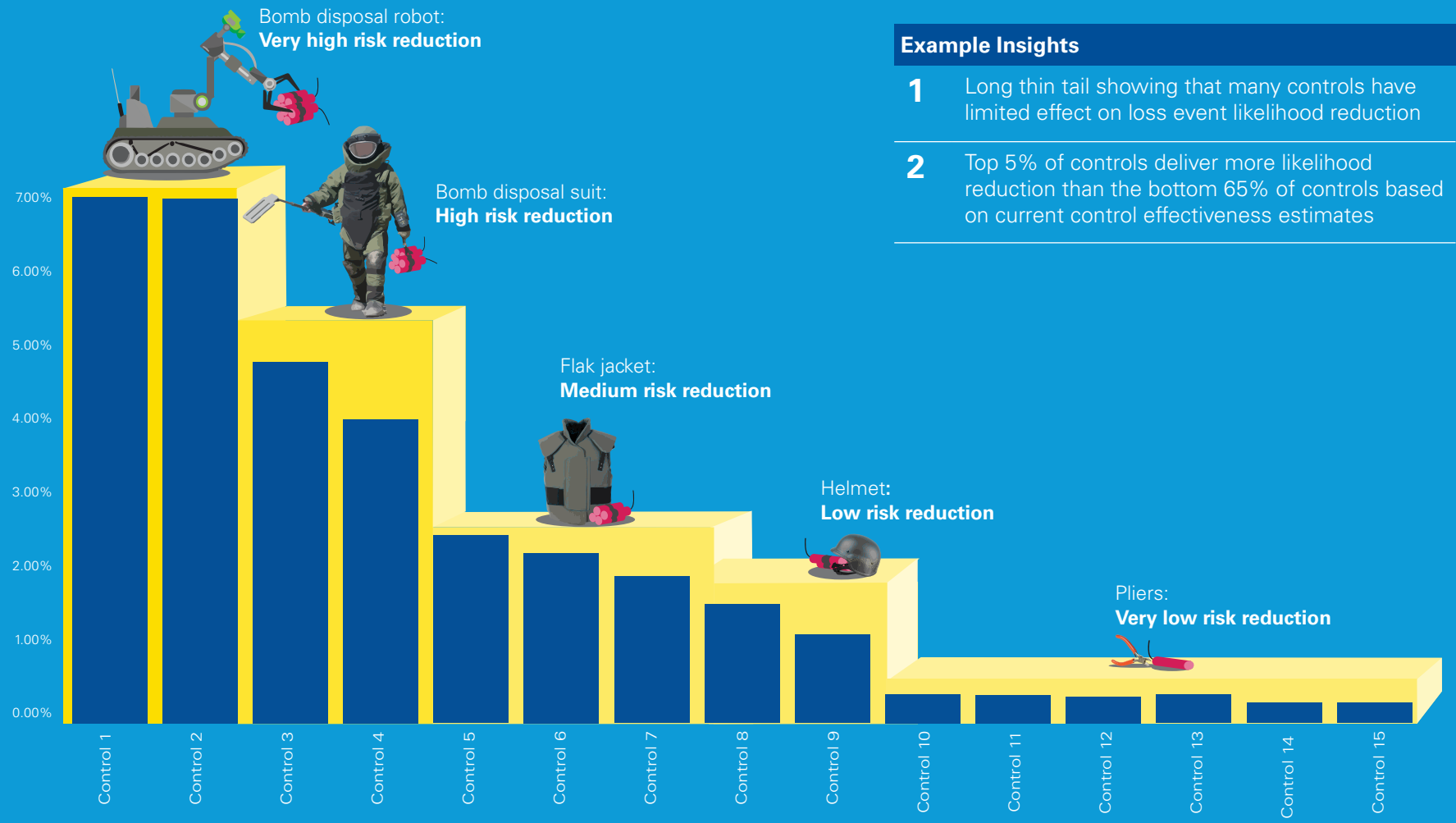
Example outputs

Control contribution to likelihood reduction

Identification of control priorities

Management have a more informed understanding of how different controls (and therefore change initiatives) vary in their contribution to reducing the likelihood of a given cyber risk scenario.

Driving the contribution to scenario % likelihood reduction is a mixture of a control's current control effectiveness and its importance in the threat scenario models.



Example Insights

1. Long thin tail showing that many controls have limited effect on loss event likelihood reduction
2. Top 5% of controls deliver more likelihood reduction than the bottom 65% of controls based on current control effectiveness estimates

The Model Realising the model's benefits

Our client has been actively using the model to support the prioritisation of the cyber transformation portfolio. It has already been an invaluable aid.

The model has been connected to a number of operational data sources in order to help automate control effectiveness estimations, and it has also been integrated into a visualisation platform in order to make it more accessible to internal stakeholders and governance committees.

The firm has been further testing the model to develop new use cases. The Cyber Security team is actively embedding the model into its existing security processes and governance framework. This will help the firm better understand how to further implement the model and to identify where its current limitations lie.

> We have already learned a lot from applying the model at the global level. And we are continuing to optimise the model by integrating new risk scenarios and further automating its inputs. We are excited about the insights this model could unlock.

Global Head of Cyber Delivery
Global Insurance Firm

The Model Realising the model's benefits

> This model has allowed us to better understand, articulate and report on our cyber risk. And that has helped us focus strategically on the most important controls, and therefore change initiatives, which help secure our business.

Global CISO
Global Insurance Firm

> Our client recognised that there are no single point solutions to managing cyber risk. It is a risk with multiple variables, with multiple answers. Our model helps to clearly and concisely deconstruct these variables to support strategic cyber decision making.

Paul Taylor
Partner, KPMG

What's next? Continued innovation...

As with any probabilistic or deterministic modelling, the accuracy of the outputs is directly correlated with the quality of the inputs. It is important to acknowledge this and its corollary: models can always be improved.

Over the coming months, KPMG will be continuing to innovate to:

- Standardise our framework so that other organisations may benefit and easily embed a cyber risk quantification capability into their BAU operations
- Enable organisations to easily improve the quality and automation of model inputs and unlock the wealth of information they already have in their environments
- Improve the coverage of data sets by exploring ways to collaborate with the community. In particular for calculating the contact rate component of our likelihood calculation

> We are committed to breaking new ground on cyber risk modelling. Whilst this paper focuses on quantifying likelihood, we plan for the next edition to de-mystify the range of £/$ impact quantification methods out there and to help explain where their value lies for cyber risk management purposes.

David Ferbrache
Global Head of Cyber Futures, KPMG

> We are proud of what we have achieved to date - blending the knowledge of real world cyber attacks with risk quantification. We are continuing to seek out new ways to innovate our model but this can be accelerated if other parties – peers, regulators and other relevant stakeholders – reach out to help us.

Konrads Klints
Director, KPMG

What's next? Call to action

We firmly believe that this model offers significant cyber risk management advantages, not only to insurers, but to those in other industries too; at its heart, the approach outlined in this paper is led by an organisation's cyber threat profile.

In this context, our goals are three-fold:

1. Provide new ideas to help improve the overall cyber risk management practice
2. Demystify cyber risk modelling and quantification for those responsible for implementing it
3. Demonstrate its value and how it can be used to support management in strategic decision making

To achieve these goals, we will seek out opportunities to share and improve our model and quantification approaches. We will engage with other leading organisations, cyber security leaders and IT leaders who have already expressed an interest in this area. We will work with relevant regulators and industry bodies. And we will look for opportunities to innovate, for example by leveraging continuous control monitoring technologies to automate control effectiveness estimations (one of the key inputs).

> We urge you to work collaboratively with us; give us your feedback and comments; share your criticisms and concerns; tell us how you would improve the model. Help us develop cyber risk modelling and quantification into a more practical, accessible and universally understood discipline.
>
> If you would like to discuss the concepts illustrated in this paper further then please do contact us.

James Hanbury
Senior Manager, KPMG

KPMG Contacts

David Ferbrache
Global Head of Cyber Futures, KPMG
david.ferbrache@kpmg.co.uk

Matthew Martindale
Partner, KPMG
matthew.martindale@kpmg.co.uk

Konrads Klints
Director, KPMG
kklints@kpmg.com.sg

James Hanbury
Senior Manager, KPMG
james.hanbury@kpmg.co.uk

Designed by CREATE | September 2020 | CRT125133A