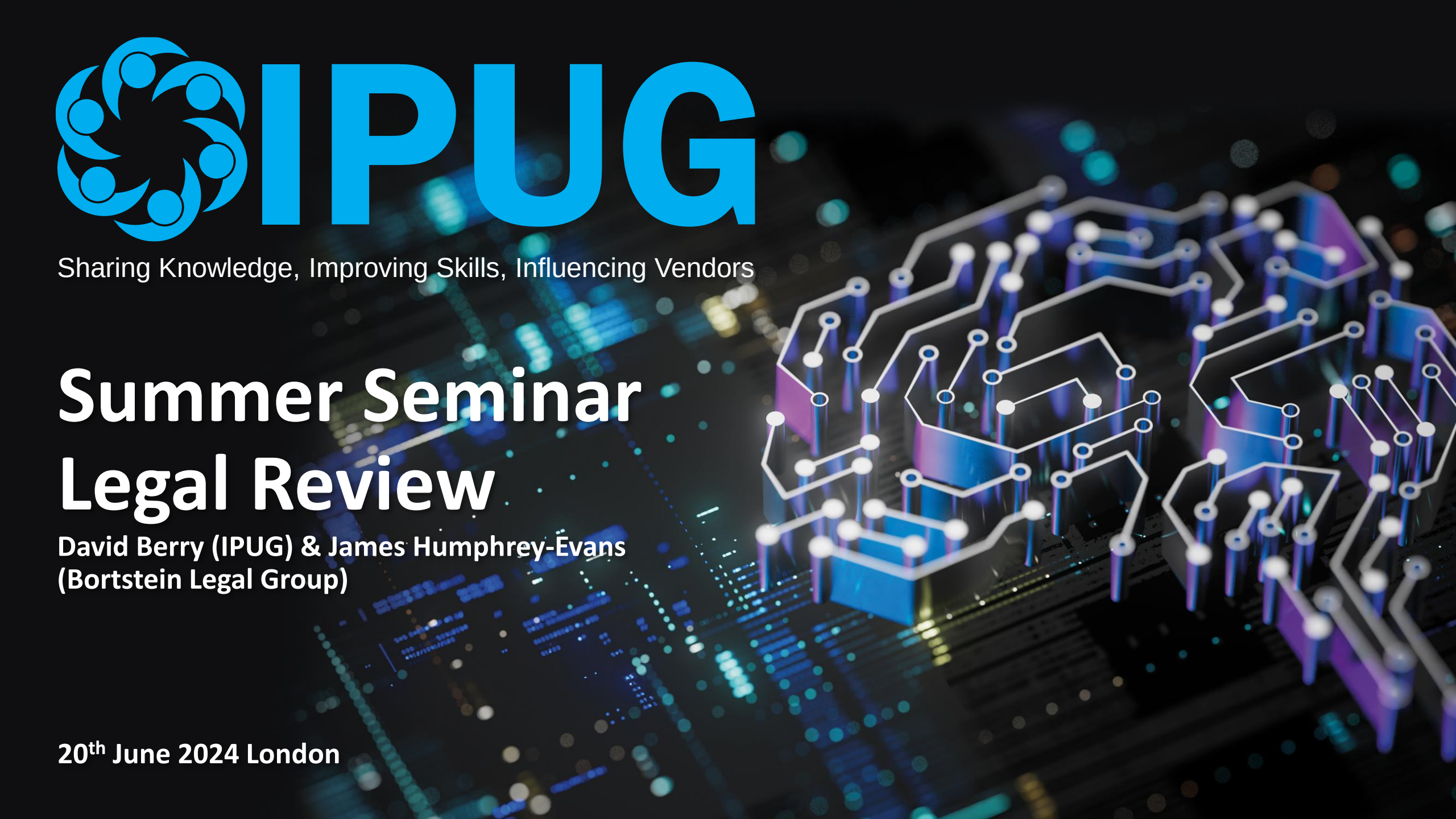
IPUG

Sharing Knowledge, Improving Skills, Influencing Vendors

Summer Seminar Legal Review

David Berry (IPUG) & James Humphrey-Evans (Bortstein Legal Group)

20th June 2024 London



Agenda

- Introduction
- Operational Resilience and DORA
- Cloud
- Use cases
- Artificial Intelligence
- ESG
- Exchange declarations and audit

Introduction to Bortstein

- Bortstein Legal Group specializes in advising financial services firms on tech, privacy and data – our clients include leading banks, brokers, insurers, investment banks and private equity.

- We have multi-lingual capabilities (including French, German, Italian, Spanish and Norwegian) and are based in London and New York

Introduction to Bortstein

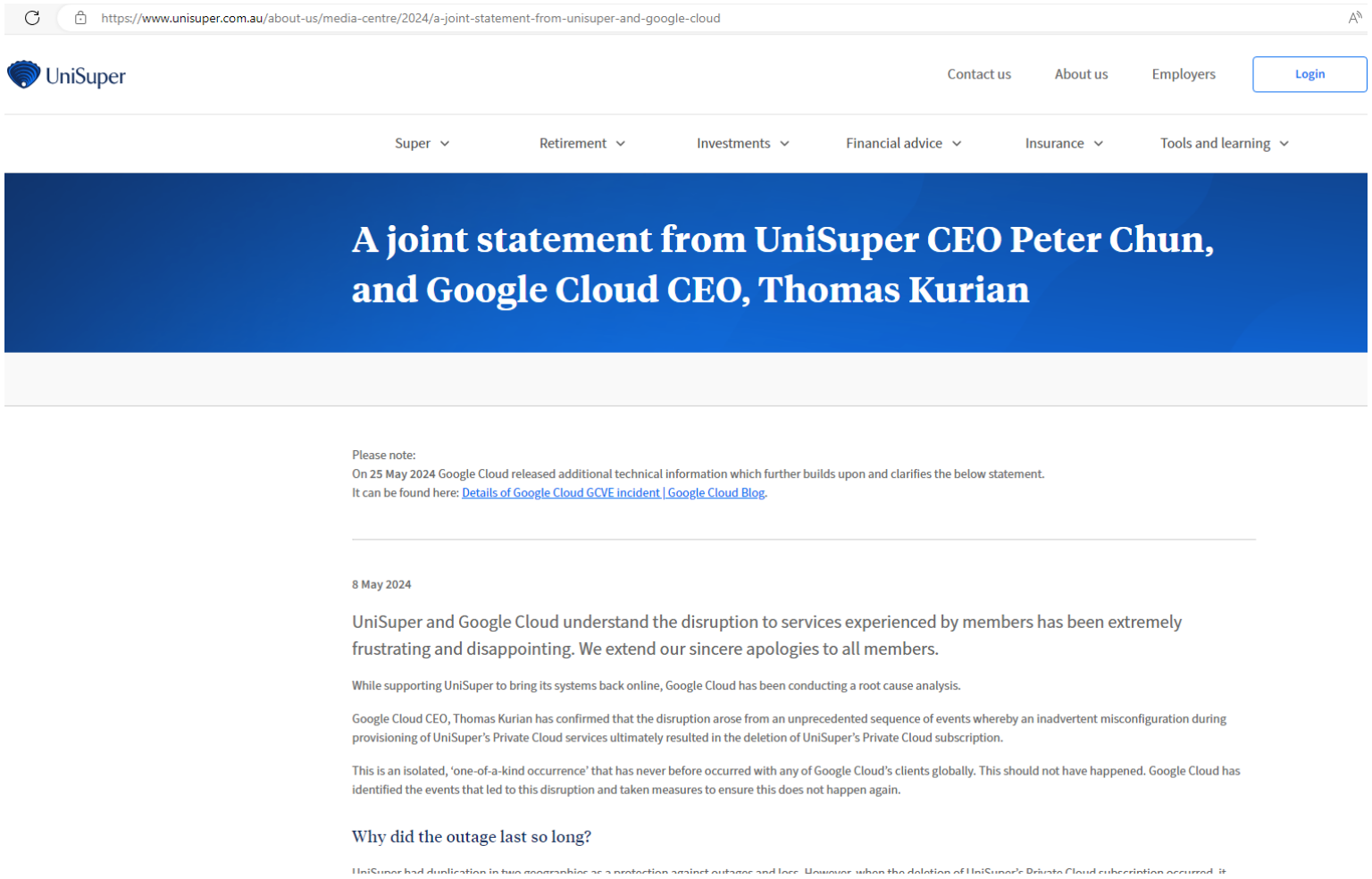
- We have dealt with numerous market data vendors, including LSEG, Bloomberg, MSCI, S&P, SIX, Moody's, Fitch, Sustainalytics, Solactive, PitchBook, FactSet, RIMES ... and many more

- We also deal regularly with large cloud providers (including AWS, Microsoft) and other tech vendors (including AI, data centre providers, telcos)

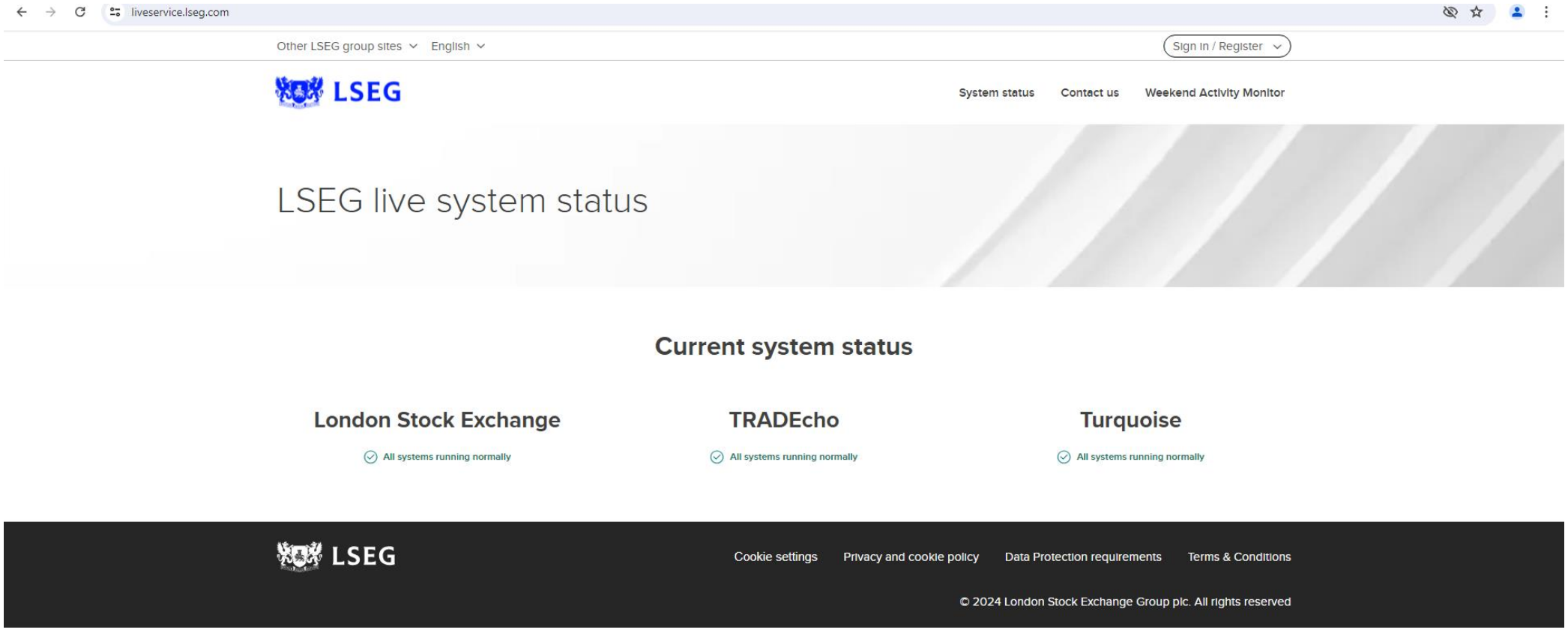
Operational Resilience

- Background of operational failures by banks (e.g. LSEG outage, ATMs not working, bank systems failures)
- European political background means that hybrid warfare could lead to attacks on financial infrastructure
- Regulators are prioritising resilience, expecting robust cybersecurity measures, including penetration testing, employee training and implementing advanced threat detection and response systems

Unisuper and Google Cloud



LSEG


liveservice.lseg.com
Other LSEG group sites
English
Sign In / Register
LSEG
System status
Contact us
Weekend Activity Monitor
LSEG live system status
Current system status
London Stock Exchange
All systems running normally
TRADEcho
All systems running normally
Turquoise
All systems running normally
LSEG
Cookie settings
Privacy and cookie policy
Data Protection requirements
Terms & Conditions
© 2024 London Stock Exchange Group plc. All rights reserved

Operational Resilience

- Even if DORA is out of scope for your institution, cybersecurity is key concern
- Market data vendors key to stability of financial markets
- Bloomberg outage caused significant problems
- Misleading / inaccurate data can affect trading, e.g. “flash crash” risk

Operational Resilience

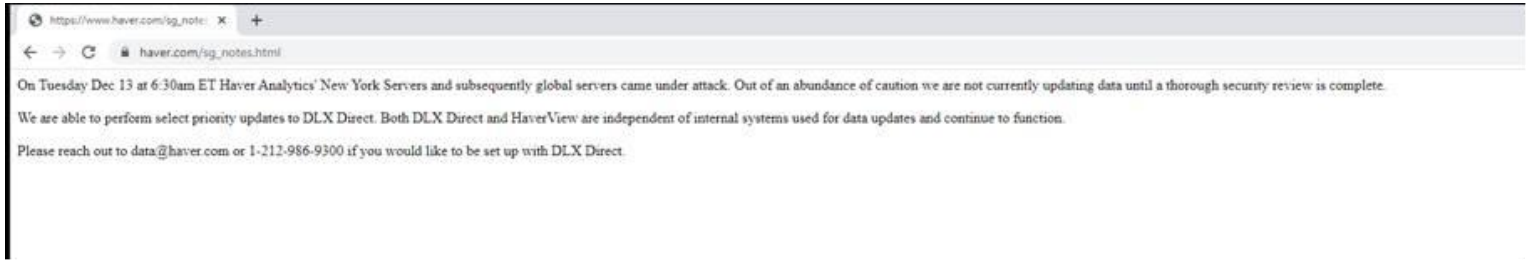
THE TRADE NEWS ALERT Working for the Bu

01 February 2023

TECHNOLOGY

ION suffers cyber attack on derivatives platform

The trading technology provider was compromised yesterday by a cyber attack t impacted its overnight processing, with some clients quarantining all communica from the firm.



Server room crash takes down Bloomberg terminals

Bloomberg denies lengthy failure was due to attackers or Coke

April 20, 2015 By: Peter Judge Comment

Archived Content

The following content is from an older version of this website, and may not display correctly.

Financial information firm Bloomberg suffered a two-and-a-half hour systems outage on Friday 17 April, cutting off hundreds of thousands of users of the firm's Bloomberg terminals.

The system was caused by "a combination of hardware and software failures", said a brief company statement. Bloomberg spokespeople ruled out a deliberate attack, and specifically denied a rumour that the failure had been caused by someone spilling a drink in a server room.

Restarting the software

The fault started around 8.30am London time, and left around 300,000 traders round the world unable to access the Bloomberg teminals which feed them with information.

The loss of the world's leading trading and data platform meant around 200 million fewer shares were sold on the London stock exchange, and the UK government's Debt Management Office

Operational Resilience

The FCA's policy statement PS 21/3 Building Operations Resilience states:

as soon as possible after 31 March 2022, and by no later than 31 March 2025, firms must have performed mapping and testing so that they are able to remain within impact tolerances for each important business service. Firms must also have made the necessary investments to enable them to operate consistently within their impact tolerances.

FCA discourages a tick-box approach

Operational Resilience

Recent FCA Guidance from 28 May 2024 does not apply to all regulated firms (applying to banks and PRA-designated investment firms, insurers, RIEs and enhanced scope SMCR payment services and e-money providers) but emphasizes need to:

- identify important business services and impact tolerances, evidenced by self-assessments
- identify vulnerabilities
- develop and keep up to date testing plans
- consider broad range of factors from the FCA Handbook
- scenario testing
- have a mature and sophisticated approach by 31 March 2025

Operational Resilience

- Cloud presents agility, scalability and disaster recovery, but potentially industry-wide single point of failure (see Google Cloud incident with Unisuper) with 3rd and nth party dependencies

- AI and machine learning: might assist resilience efforts by anticipating disruptions and automating recovery processes (but can also present security risks)

- See: https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence

DORA

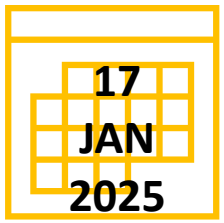
On 27 December 2022, the regulation on digital operational resilience for the financial sector (also known as the "**Digital Operational Resilience Act**" or "**DORA**") was officially published in the EU Official Journal, resulting in the introduction of new resilience obligations relating to technology and cyber being introduced for financial entities.

DORA includes requirements regarding how firms must manage information and communications technology ("ICT") risk, both within its organization and with respect to its use of any ICT third-party vendor.

ICT services are defined in broad terms in Article 3(21):

"digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services."

Obligations will apply from **17 January 2025.**



The 5 “pillars’ of DORA

1. ICT risk management (Chapter II DORA)

- Set of key principles and requirements on ICT risk management framework

2. ICT-related incident reporting (Chapter III DORA)

- Harmonise and streamline reporting + extend reporting obligations to all financial entities

3. Digital operational resilience testing (Chapter IV DORA)

- Subject financial entities to basic testing or advanced testing (e.g. TLPTs)

4. ICT third-party risk (Chapter V DORA)

- Principle-based rules for monitoring third-party risk, key contractual provisions + oversight framework for critical ICT TPPs

5. Information sharing

- Voluntary exchange of information and intelligence on cyber threats

DORA

- Even if your firm does not operate in the EU, so the Digital Operational Resilience Act (DORA) will not directly apply. EU clients however may need to have assurances that the operational capabilities of a non-EU firm are robust
- Financial sector increasingly dependent on technology / tech companies for provision of financial services
- DORA seeks to embed resilience as key practice across financial entities in the EU
- DORA builds on previous EU regulatory regimes by creating legal obligations (rather than guidelines) and expands scope to cover all technology and financial firms

DORA

- Even if your firm does not operate in the EU, so the Digital Operational Resilience Act (DORA) will not directly apply. EU clients however may need to have assurances that the operational capabilities of a non-EU firm are robust
- Financial sector increasingly dependent on technology / tech companies for provision of financial services
- DORA seeks to embed resilience as key practice across financial entities in the EU
- DORA builds on previous EU regulatory regimes by creating legal obligations (rather than guidelines) and expands scope to cover all technology and financial firms

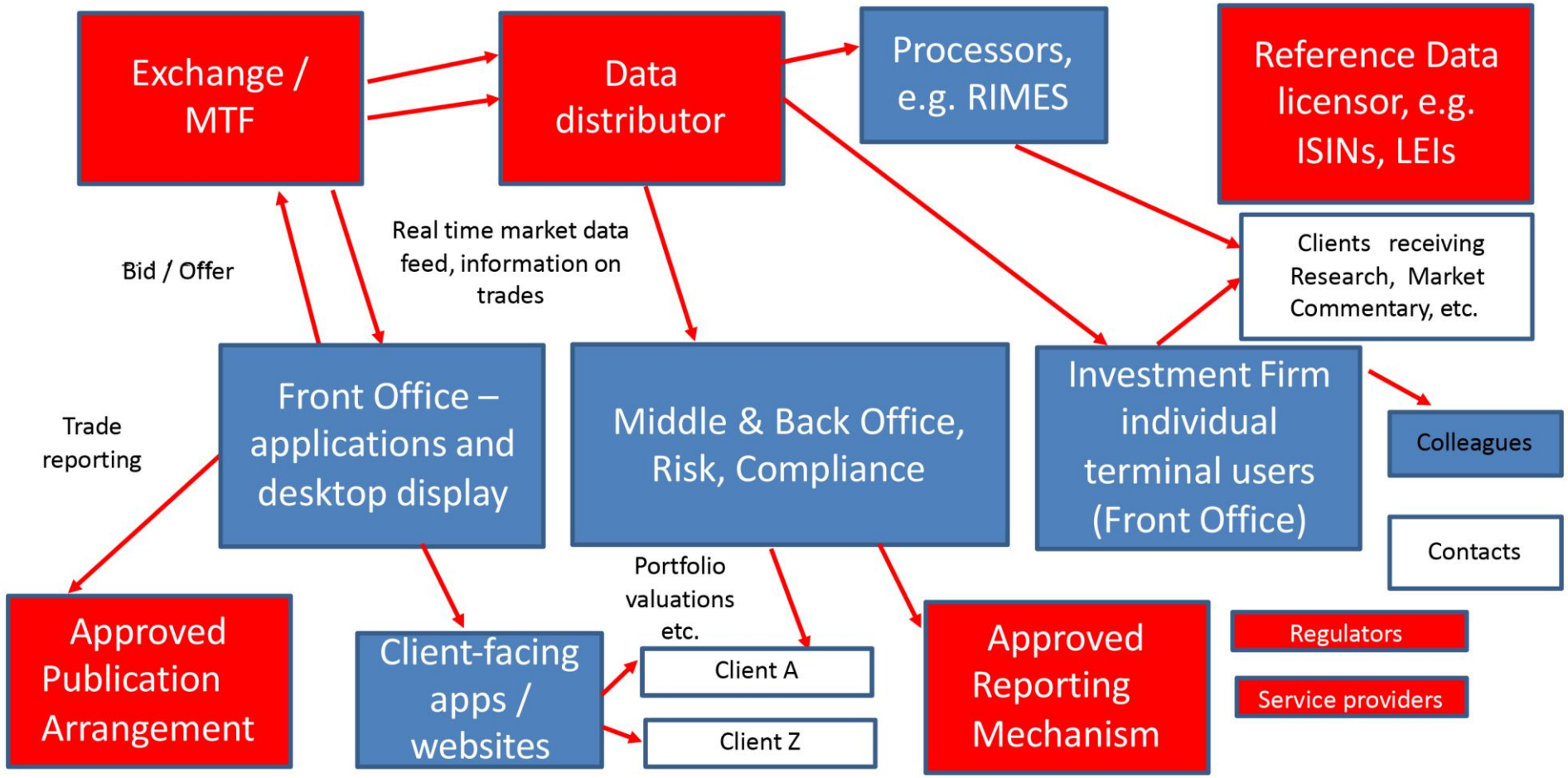
SIFMA / Bortstein Legal Group whitepaper on cloud and regulation

https://www.sifma.org/resources/general/navigating-regulatory-challenges-in-cloud-services-agreements/

Use cases in market data contracts

- Vendors in market data are often reluctant to make changes, but most will accept “nudges” on key points
- Look out for use case (and prohibitions)
- Identify what the contract is – a contract may have many components

Key issue: data flows often complex

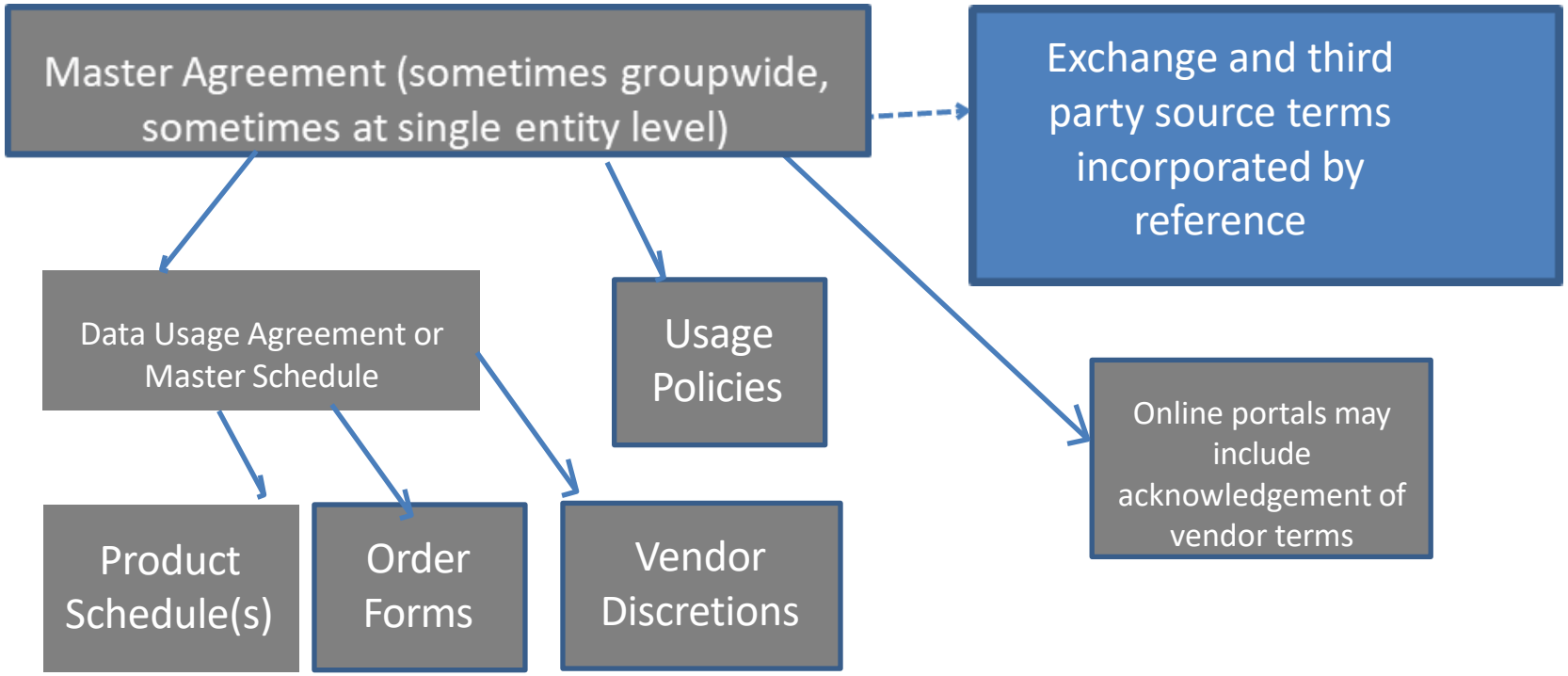


Cloud may be seen as separate use case

- Old agreements sometimes very prescriptive on hardware
- Cloud usage may be subtly prohibited in legacy agreements
- Insert positive permission to use cloud (ideally in master agreement so that it cascades to order forms and schedules)

The order form is often the tip of the iceberg

Structures of vendor contracts vary



Multiple order forms or product schedules possible – these are often key to understanding permitted use case

“Top Dozen” points

Pricing (and how pricing can change)	Use case (especially for group enterprises, use of AI, external usage, how deployed)
Use and sharing of small extracts internally and externally	Derived Data (including reporting to clients/regulators as needed)
Keeping data for regulatory purposes and keeping derived data after end of subscription	Ability to share data with regulators and their agents and under freedom of information requests
Protecting information and personal data	Understanding product governance (especially ESG and research)
Ability for vendor to change terms	Information security
Audit rights (and limiting / removing them)	Indemnity against infringement claims

Some examples from practice

1. KYC / AML vendor: deletion of data on termination
2. Order form autorenewed even though vendor was in active discussions about the changes needed for new term (often wise to get termination notice in early to prevent autorenewal)
3. Authorised corporate directors use chargeable separately to issuers
4. Use of data by SPVs (not affiliates)
5. Inventory and risk data of customer belongs to SaaS provider
6. Packages of data sold by SaaS vendor as “one stop shop” with inadequate licences

Artificial Intelligence

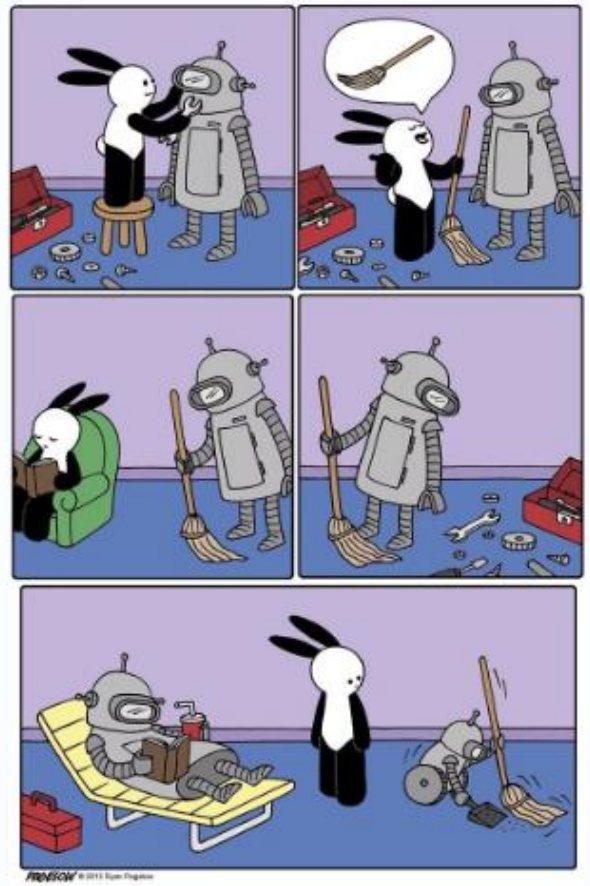
First Person: Jeremy Mabbitt

'I helped cause the credit crunch'

Jeremy Mabbitt's software helped create the complex investments that fuelled the banking crisis © FT

As told to Maike Currie AUGUST 3 2012

Whenever I watch those movies and documentaries about the credit crunch, and the endless debates about who or what caused it, I'm amazed that no one ever mentions Galapagos. Galapagos was the software used by most investment banks to create the complex investment products known as collateralised debt



AI: What is it?

- AI term first used in 1956, but entered the general vocabulary and everyday life more recently
- AI used in trading apps in the early 2000s
- Everyone had fun with GPT and Dall-E, but now embedded in more routine office IT (Copilot, Bing, LinkedIn)

AI: What is it?

ChAI Insight

Palantir

Definition of AI in EU AI Act

- “AI system” means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

What are users' needs?

- Use AI to stay competitive
- Save money and time
- Useful insights and data (so check derived data wording too)
- Comply with laws and regulations (including EU AI Act and privacy legislation – scope for large penalties)

Vendors and AI

MARKET DATA

CME Group Data Services Advisory Notices

INTERNAL CONTROLS REQUIRED: USE OF CME GROUP DATA IN ARTIFICIAL INTELLIGENCE SOLUTIONS

Updated February 2024

Please note that unless otherwise defined herein in, any capitalized terms shall have the same meaning as set out in the Information License Agreement. Please see Appendix A for a glossary of terms for purposes of this Advisory Notice.

This CME Group Data Services Advisory Notice is being issued on January 31, 2024, to remind Licensees and Subscribers to CME Group Information ("Information") of their obligation to maintain effective Internal Controls as it relates to access of Information pursuant to CME Group's Information Policies, Information License Agreement ("ILA") (and its Schedules) and Subscriber Addendum.

CME Group requires all Licensee Group and Subscriber Group entities to have and to maintain, at all times, effective Internal Controls and, as part of having effective Internal Controls, use an entitlement system that manages entitlement, access and distribution of Information. Internal Controls must be able to monitor and control the downstream flow of Information from each data feed point to all applications, application users, and recipient Devices within a Licensee Group or Subscriber Group entity. These systems must ensure that only those applications, solutions, the application users, and their Devices that are entitled and licensed to receive access to the Information can do so. Access to Information that is not otherwise governed by effective Internal Controls is strictly prohibited.

Licensee Group and Subscriber Group entities must pay particular attention to ensure proven and appropriate Internal Controls are in place to govern Artificial Intelligence and subsets of Artificial Intelligence which include, but are not limited to Machine Learning, Deep Learning, Generative Artificial Intelligence, Large Language Models, and generative pre-trained transformers (also known as GPT) (collectively "AI Solutions"), that have access to Information. Training of AI Solution Models using Information must strictly adhere to the terms and conditions of the ILA, Subscriber Addendum, and Information Policies, including the maintaining of appropriate licenses. Moreover, bona fide Internal Controls are required to govern all downstream access to Information – including distribution outside the Licensee or Subscriber Group – or works derived from Information (also known as derived data or derived works) via AI Solutions, no matter the means with which an application, application user or Device calls, queries, or otherwise has access to the Information.

The text of **Section 2** of the **Information Policies** is set forth below and asserts a Licensee Group or Subscriber Group's responsibilities as it relates to Internal Controls.

2. Internal Controls

2.1. Internal Controls must meet the following requirements:

a) Account for all Units of Count that have been technically enabled to access or receive Information;

b) Provide accurate historical audit trail information;

c) Generate audit trail reports, showing software-controlled entitlements (not administrative reports), including activations and deactivations;

d) Govern Device access with unique ID and password combinations that are not shared;

e) Prevent, or identify and count, simultaneous entitlement or access to Information, by the same unique ID and password combination; and

f) Are used to govern Licensee and Subscriber use of Information.

CME Group

What are vendors' concerns?

- Monetize additional use cases for their data
- Retain market position
- Prevent copies of their data being redistributed and used

The New York Times | https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work

Millions of articles from The New York Times were used to train chatbots that now compete with it, the lawsuit said.

By Michael M. Grynbaum and Ryan Mac

Dec. 27, 2023

The New York Times sued OpenAI and Microsoft for copyright infringement on Wednesday, opening a new front in the increasingly intense legal battle over the unauthorized use of published work to train artificial intelligence technologies.

The Times is the first major American media organization to sue the companies, the creators of ChatGPT and other popular A.I. platforms, over copyright issues associated with its written works. The lawsuit, filed in Federal District Court in Manhattan, contends that millions of articles published by The Times were used to train automated chatbots that now compete with the news outlet as a source of reliable information.

Sample data vendor clauses

“Client shall not use licensed Information hereunder in connection with artificial intelligence, black box, machine learning/processing or algorithmic trading applications.”

Sample Exchange AI Definitions

- **Glossary of AI terms – supplied by each Trading Venue / Exchange - to be clearly "learned" by IPUG members to define their applications usage pattern**

- **Artificial Intelligence (AI): A field of computer science where computers emulate human thought and perform tasks in real-world environments.**
- **Machine Learning (ML): A type of Artificial Intelligence that is used to identify patterns, make decisions, and improve through training data and experience.**
- **Deep Learning: A type of Machine Learning that uses neural networks with multiple layers of neurons to model and solve problems**
- **Generative AI: A type of Deep Learning whereby Models can be used to generate new content based on data used to Train the Models, wherein the new content can include audio, code, images, text, simulations, and videos**
- **Large Language Model: Models that can recognize, summarize, redistribute, translate, predict, and generate text using very large datasets**
- **Model: A program that is trained on a set of data to recognize patterns**
- **Train: A process of providing access to data to teach a Model to perceive, interpret and learn from data**

Sample Exchange AI Licensing 1

- **IPUG Members must link the AI Definitions and their usage pattern for each application (in ACM/ILM/MDM/FITS) with the Trading Venue/Exchange associated licensing BEFORE engaging in the data usage…**

- **Use of Historical Information**
- **Requires effective Internal Controls to prevent unauthorized redistribution of the Information without the appropriate license.**
- **Requires effective Internal Controls to prevent the distribution of any derived works of the Information without the appropriate license.**

- **Use of Delayed Information**
- **Requires appropriate Non-Display licenses.**
- **Requires effective Internal Controls to prevent unauthorized redistribution of the Information without the appropriate license.**
- **Requires effective Internal Controls to prevent the distribution of any derived works of the Information without the appropriate license.**

Sample Exchange AI Licensing 2

- Use of Real-Time Information

- **Requires appropriate Non-Display licenses.**

- **Requires effective Internal Controls to prevent unauthorized redistribution of the Information without the appropriate license.**

- **Requires effective Internal Controls to prevent the distribution of any derived works of the Information without the appropriate license.**

- **Requires effective Internal Controls including an appropriate entitlement system acceptable to the Trading Venue/Exchange (and its auditors at a later date…) that is able to monitor and control the downstream flow of Information to all applications, application users and Devices within a Licensee Group (See Trading Venue/Exchange Information Policy Requirements for Entitlement Systems). The entitlement systems must ensure that only those applications, the application users, and their Devices that are entitled and licensed to access the Information can do so.**

- **Example: https://www.cmegroup.com/files/download/ai-data-services-advisory.pdf**

Scraping Technology Limitation

- Use of Scraping by IPUG members on – so called – public data displayed by exchanges (See EDI whitepaper to SEC on historical data acquired by a Trading Venue / Exchange)

- Trading Venue / Exchange policy reminder:

- This is a reminder that scraping of data from any part of the Trading Venue / Exchange or affiliated websites is strictly prohibited.

- Use of scraping tools including but not limited to bots, crawlers, spiders, or any other scraping solutions to capture Trading Venue / Exchange information from the Trading Venue / Exchange website is not allowed per Trading Venue / Exchange ’s Data Terms of Use.
- -> IPUG members need to check it every time

Key points for deals with AI vendors

- Will your data be used to educate a third party's Large Language Model? (Hopefully not?)
- Will your data be protected from viewing by anyone else? (Hopefully yes !)
- Where will your data be held?
- What security measures will be in place to protect your data?
- Ownership of input, intermediate and output data

ESG data governance

ESG

- Seek assurance around methodology
- Audit right for customer over compliance with methodology?
- Scepticism over ESG data
- Interesting read: https://www.bloomberg.com/graphics/2021-what-is-esg-investing-msci-ratings-focus-on-corporate-bottom-line/

Audit

- Preparation
- NDA
- Scope of audit
- Audit often based on inaccurate assumptions
- Control communications
- Protect IT staff from auditor queries
- Challenge incorrect findings

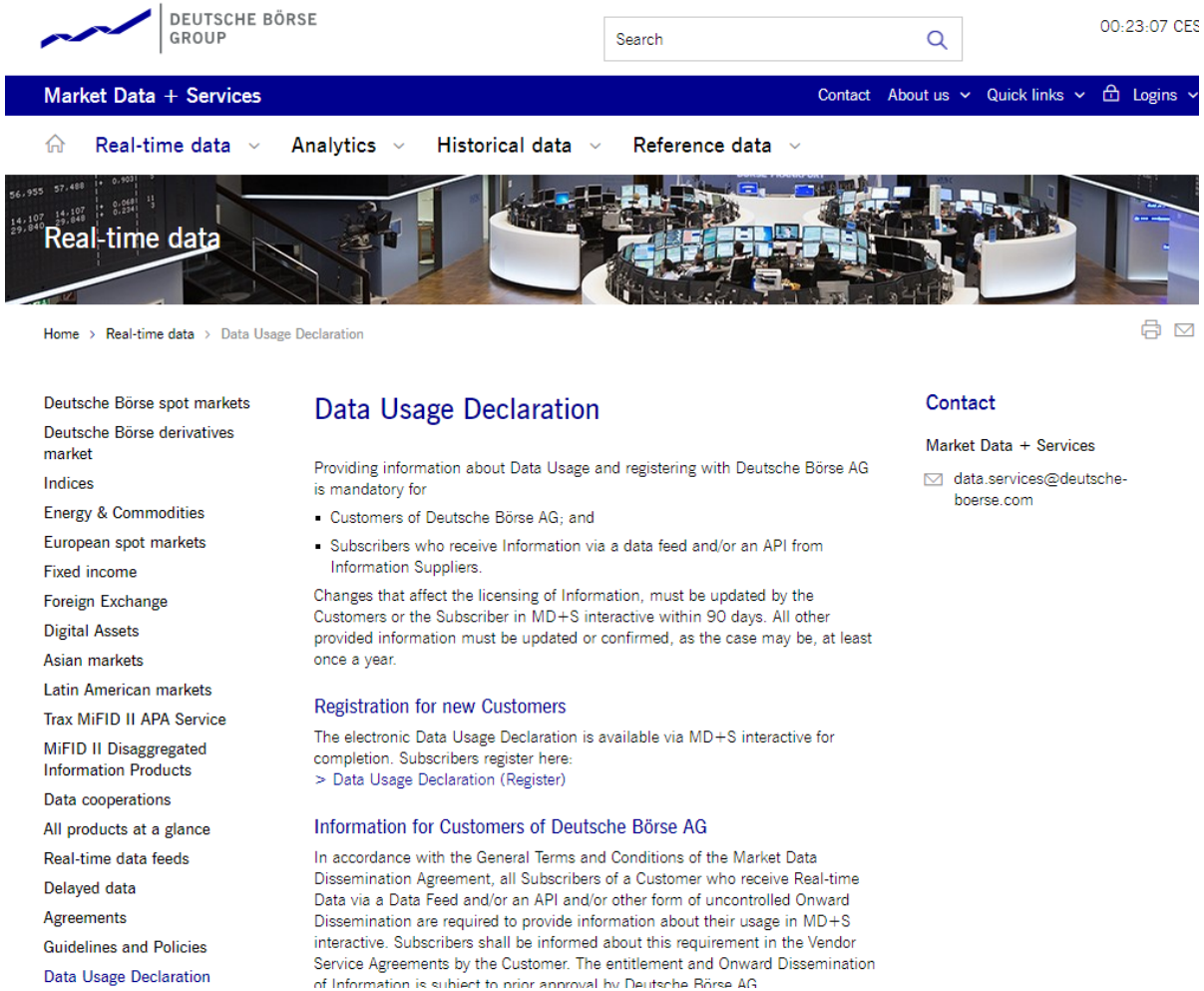
Audit Clauses on Open Source

- **Service Usage & Open Source:** *(Text below extracted from the Vendor contract)*

- If Vendor provides any development materials or documentation as part of the *Services* (collectively,
- "*Development Materials*"), the Client Firm may use such Development Materials only internally for the Client Firm's use of the *Services* in accordance with this Schedule and may not
- (1) share, disclose or otherwise make available such Development Materials to any third party and/or
- (2) use the Development Materials in any manner that would cause the Materials to become subject to any "open source license" (*i.e.,* a license that creates or purports to create obligations that other software incorporated into, derived from or distributed with the licensed materials be
- (A) disclosed or distributed in source code form,
- (B) licensed for the purpose of making derivative works, or
- (C) redistributable at no charge.

- **-> IPUG Members note: Open Source Third Party usage is free but access is chargeable with some vendors**

Exchange declarations



References

- https://www.sifma.org/resources/general/navigating-regulatory-challenges-in-cloud-services-agreements/
- PS21/3 Building operational resilience | FCA
- Operational resilience: insights and observations for firms | FCA
- Digital Operational Resilience Act (DORA) - European Union (europa.eu)
- https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence

Discussion

Any questions?

Please feel free to contact me at
jhumphreyevans@blegalgroup.com

NOTICE AND DISCLAIMER: This presentation is intended to provide a structure for a brief discussion of selected relating to market data contracts only for attendees of the IPUG Summer Seminar in June 2024. Market data, IT and related legal and regulatory matters are broad and complex topics. This presentation is for review only and is not legal or technical advice. This presentation is therefore neither comprehensive nor tailored to individual needs. Neither the presenters, IPUG nor Bortstein LLP shall be liable in any way for any losses, damages or other consequences of using this presentation, which may be incomplete, inaccurate or out-of-date. You should consider obtaining appropriate commercial, IT and legal advice when considering market data requirements. Please do not copy or forward without permission from the presenters.

20th June 2024 London

Biography

James Humphrey-Evans

James Humphrey-Evans is an established expert in the areas of outsourcing, procurement, technology, e-commerce and governance matters, with a focus on the needs of financial services clients. Prior to joining the firm, James was a director in the legal department of MUFG Securities, which he joined after having similar roles at Nomura, Lehman Brothers and Barclays.

James' extensive experience allows him to quickly bring parties to resolution on the myriad issues that typically arise in complex technology transactions. Over the years, he has provided close daily support to in-house procurement, operations and technology teams, as well as front office business teams, assisting them in achieving their commercial and risk management goals on numerous software, cloud, consultancy, market data, index licensing, data center and other transactions, in addition to helping organizations comply with regulatory requirements affecting IT and operations functions. James obtained the CIPP/E qualification for GDPR from the International Association of Privacy Professionals. James speaks frequently at industry events.

James graduated from King's College London with LL.B. First Class Honours, having spent two semesters studying Law at the University of Passau, Germany. James also holds an LL.M. degree from the University of Cambridge and was from 2003-2009 a guest lecturer at the University of Münster, Germany. James practises as a lawyer in England & Wales and, while not practising in Ireland, is qualified as a solicitor in Ireland.

Career History

Bortstein Legal Group
Partner
2013 -

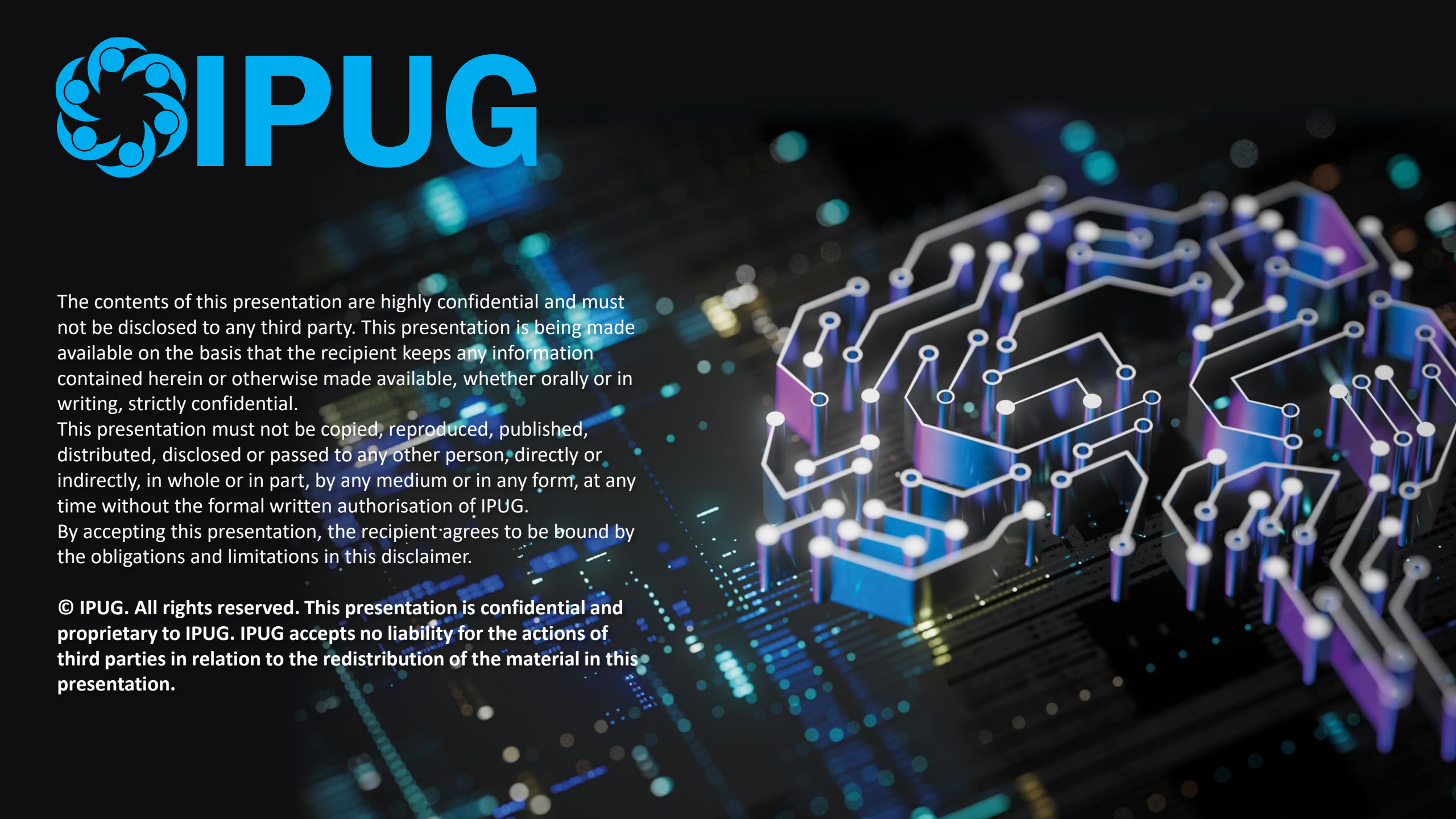
Mitsubishi UFJ Securities
Director, Legal
2010 - 2013

Nomura
2008 - 2010

Lehman Brothers
2008

Barclays
2004 - 2008

A&O
1999 - 2004



The contents of this presentation are highly confidential and must not be disclosed to any third party. This presentation is being made available on the basis that the recipient keeps any information contained herein or otherwise made available, whether orally or in writing, strictly confidential.
This presentation must not be copied, reproduced, published, distributed, disclosed or passed to any other person, directly or indirectly, in whole or in part, by any medium or in any form, at any time without the formal written authorisation of IPUG.
By accepting this presentation, the recipient agrees to be bound by the obligations and limitations in this disclaimer.