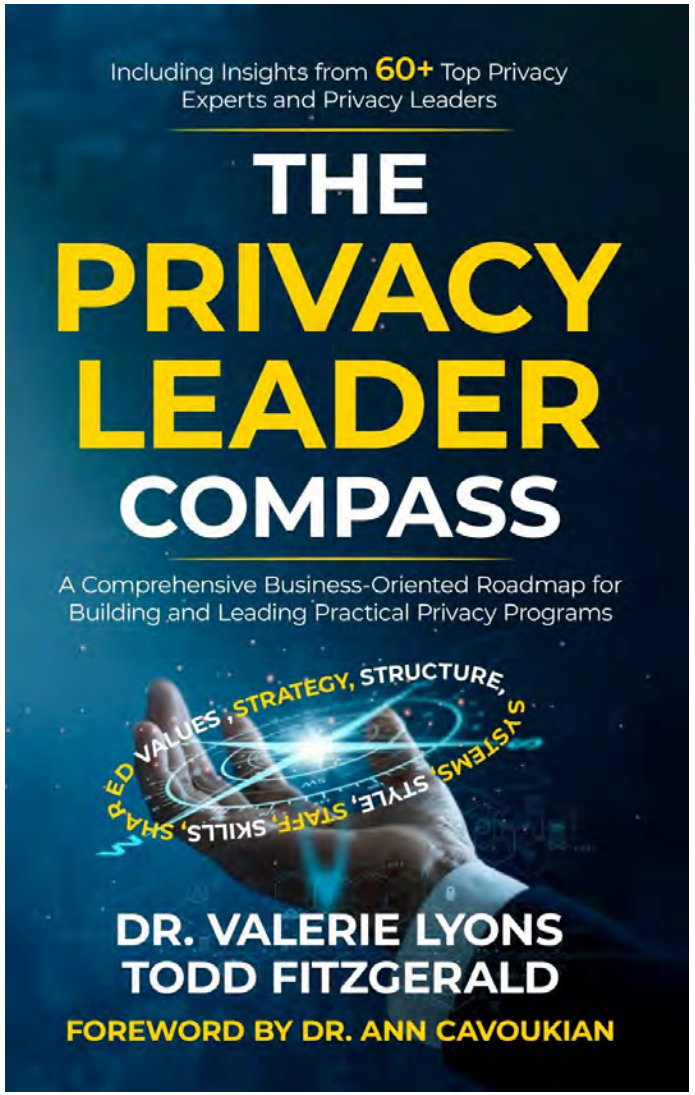
Institute of Directors Ireland

Digital Governance: AI, Cybersecurity, and Privacy

with Dr. Valerie Lyons, Company Director, and Chief Operating Officer, BH Consulting

20th March 2025



edpb
European Data Protection Board

BHConsulting
Cybersecurity & Data Protection

AGENDA

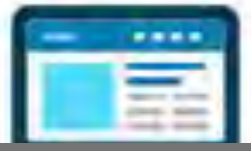
- Privacy & Data Protection Vs Cybersecurity
- Cybersecurity and Data Protection
- NIS2 & CRA
- AI Governance
- Why emerging tech presents such risks?

BHConsulting
Cybersecurity & Data Protection

Privacy Vs Data Protection Vs Cybersecurity?

CYBERSECURITY – INFOSEC CIA TRIAD

Safeguarding the accuracy and completeness of information and processing methods.



"Organisational and Technical Measures"

Information Security (System)

Includes:

- Protection from unauthorized access and use;
- Protecting data on systems, in transit, in process,...

Confidentiality

Availability

Includes controls for:

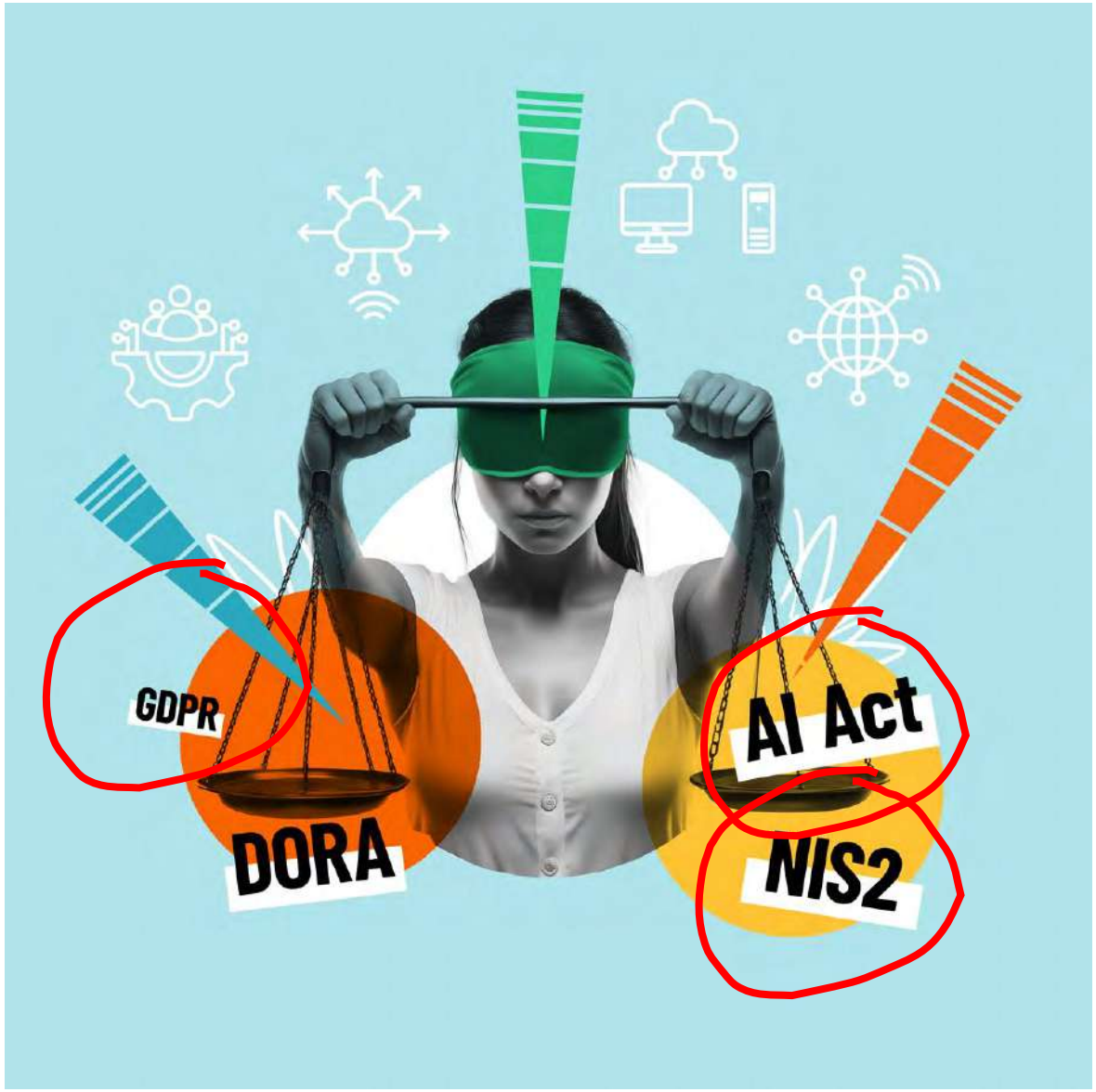
Acceptable level of performance
Fault tolerance
Prevention of data loss and destruction
Reliable backups, redundancy,...

Cyber Resilience Act

Data Act

Data Governance Act

Digital Services Act



NIS2 DIRECTIVE: Focuses on ***cybersecurity risk management and incident reporting for essential and important entities*** (e.g., energy, healthcare, digital infrastructure) to enhance the resilience of critical services.

CYBERRESILIANCE ACT(CRA): ***Security requirements on hardware and software products*** (e.g., IoT devices, operating systems) to ensure cybersecurity is built into products from the design phase.

ISO 27001 - Cyber
ISO 27701 – Privacy/DP
ISO 42000 – AI Gov

NIST CyberSecurity Framework
NIST Privacy Framework
NIST AI Governance Framework

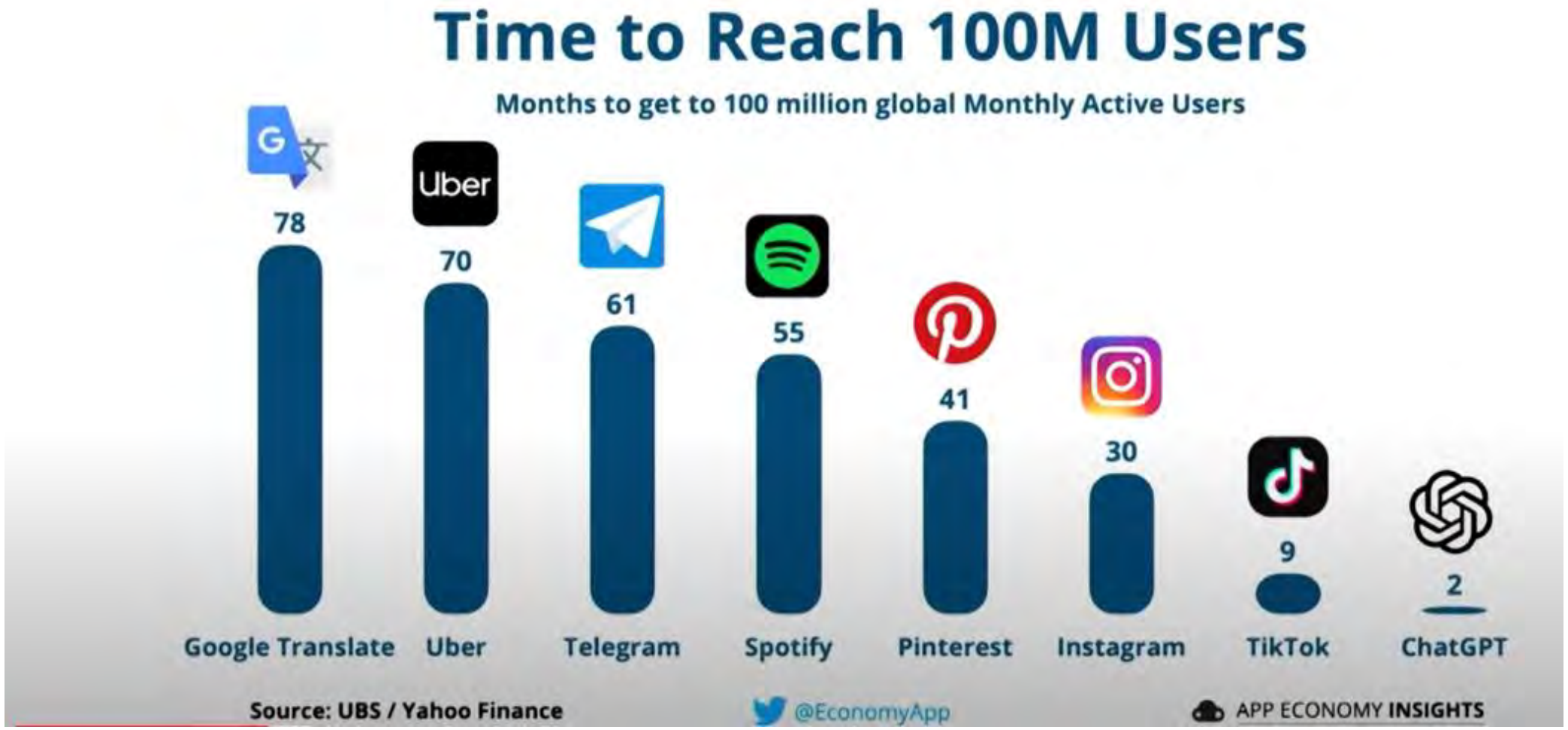
PCI DSS – Cyber & DP
EU Cloud Code of Conduct – DP

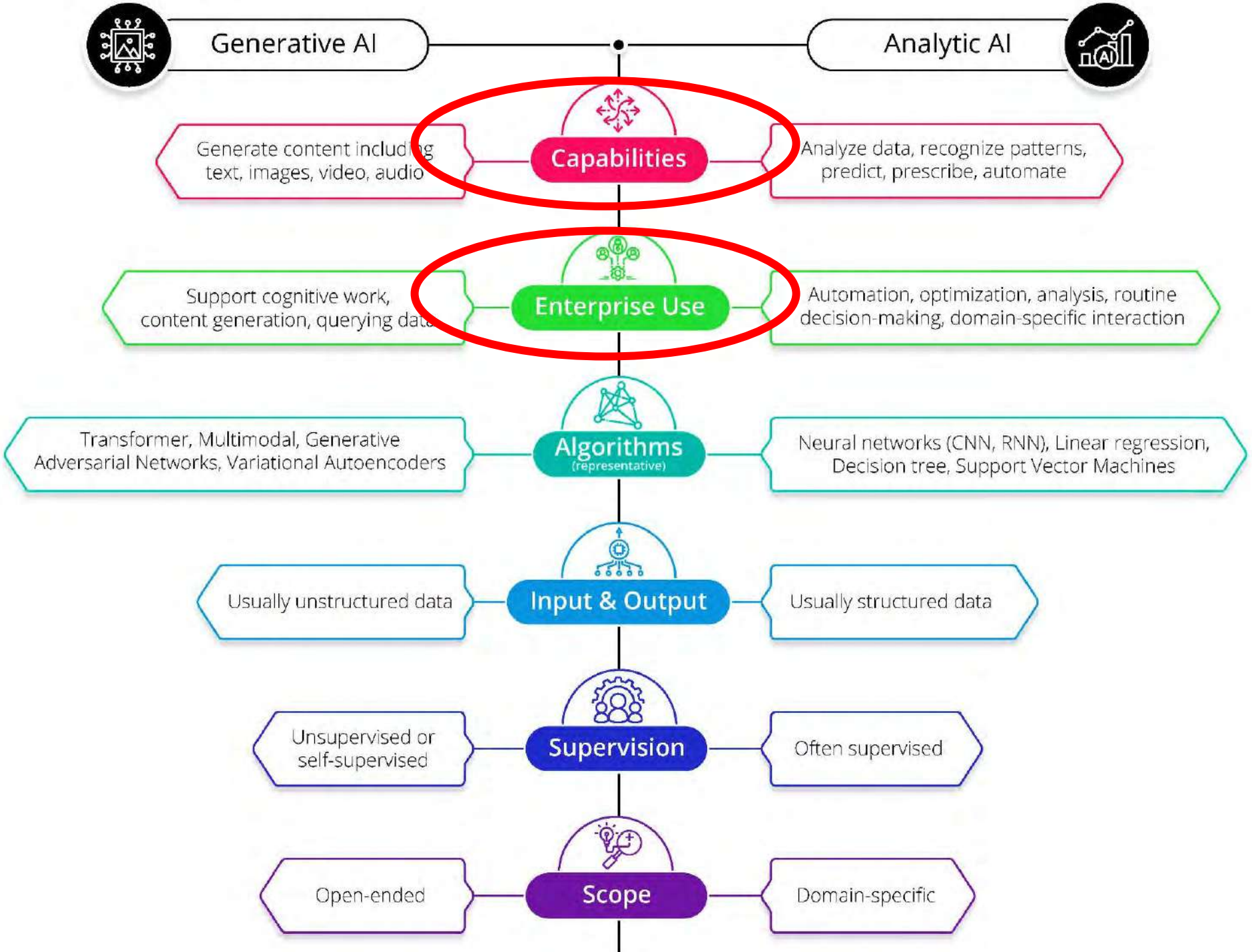
Digital Trust Framework – Cyber & DP

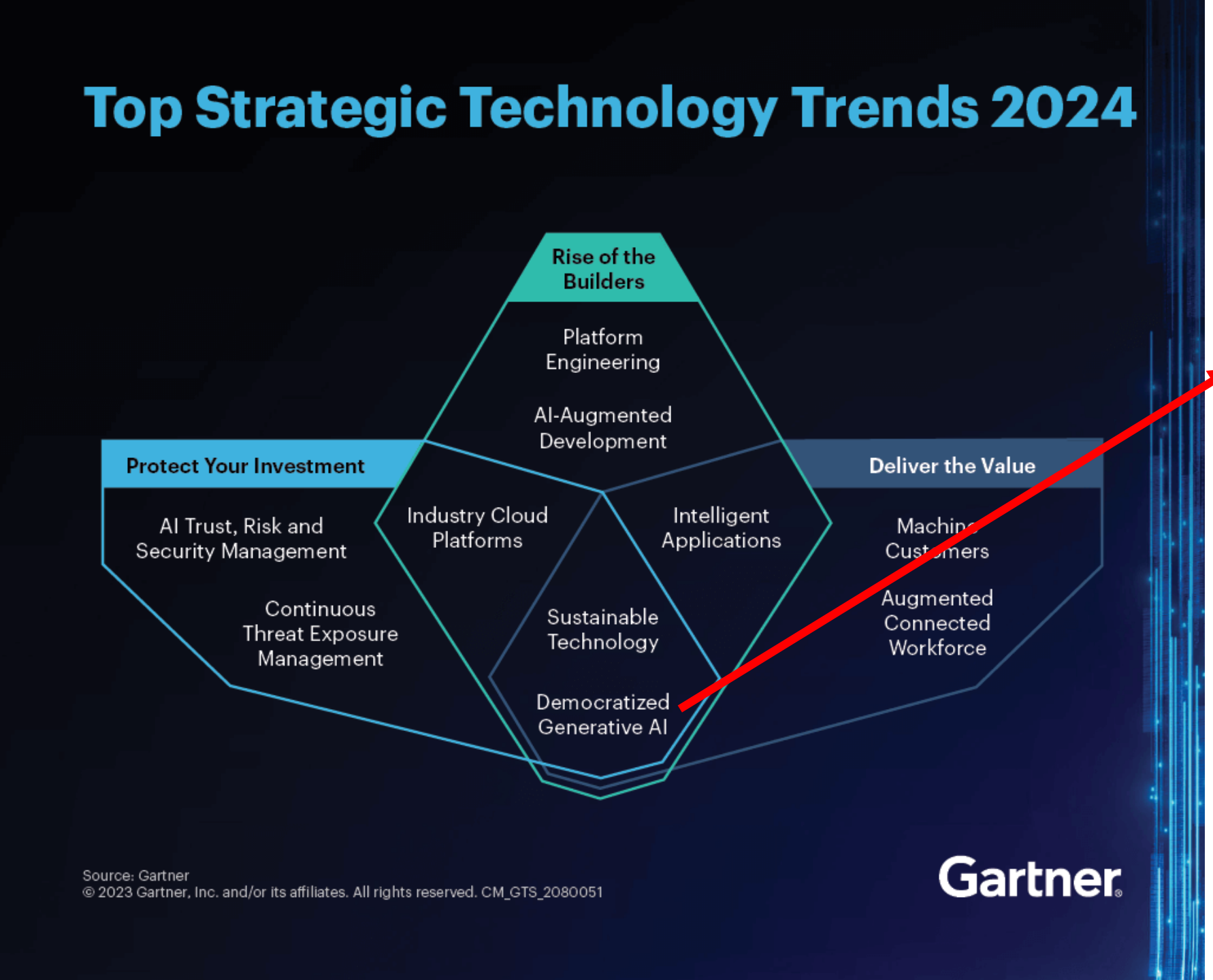
AI Governance….

BHConsulting
Cybersecurity & Data Protection

How Long Has AI Been Around?




Generative AI
Analytic AI
Capabilities
Generate content including text, images, video, audio
Analyze data, recognize patterns, predict, prescribe, automate
Enterprise Use
Support cognitive work, content generation, querying data
Automation, optimization, analysis, routine decision-making, domain-specific interaction
Algorithms
(representative)
Transformer, Multimodal, Generative Adversarial Networks, Variational Autoencoders
Neural networks (CNN, RNN), Linear regression, Decision tree, Support Vector Machines
Input & Output
Usually unstructured data
Usually structured data
Supervision
Unsupervised or self-supervised
Often supervised
Scope
Open-ended
Domain-specific



The combination of cloud computing, open source, pre-trained models democratizes GenAI, making these models available to workers everywhere.

According to Gartner, more than 80% of businesses will have implemented GenAI APIs by 2026.

EU Artificial Intelligence Act: Risk levels

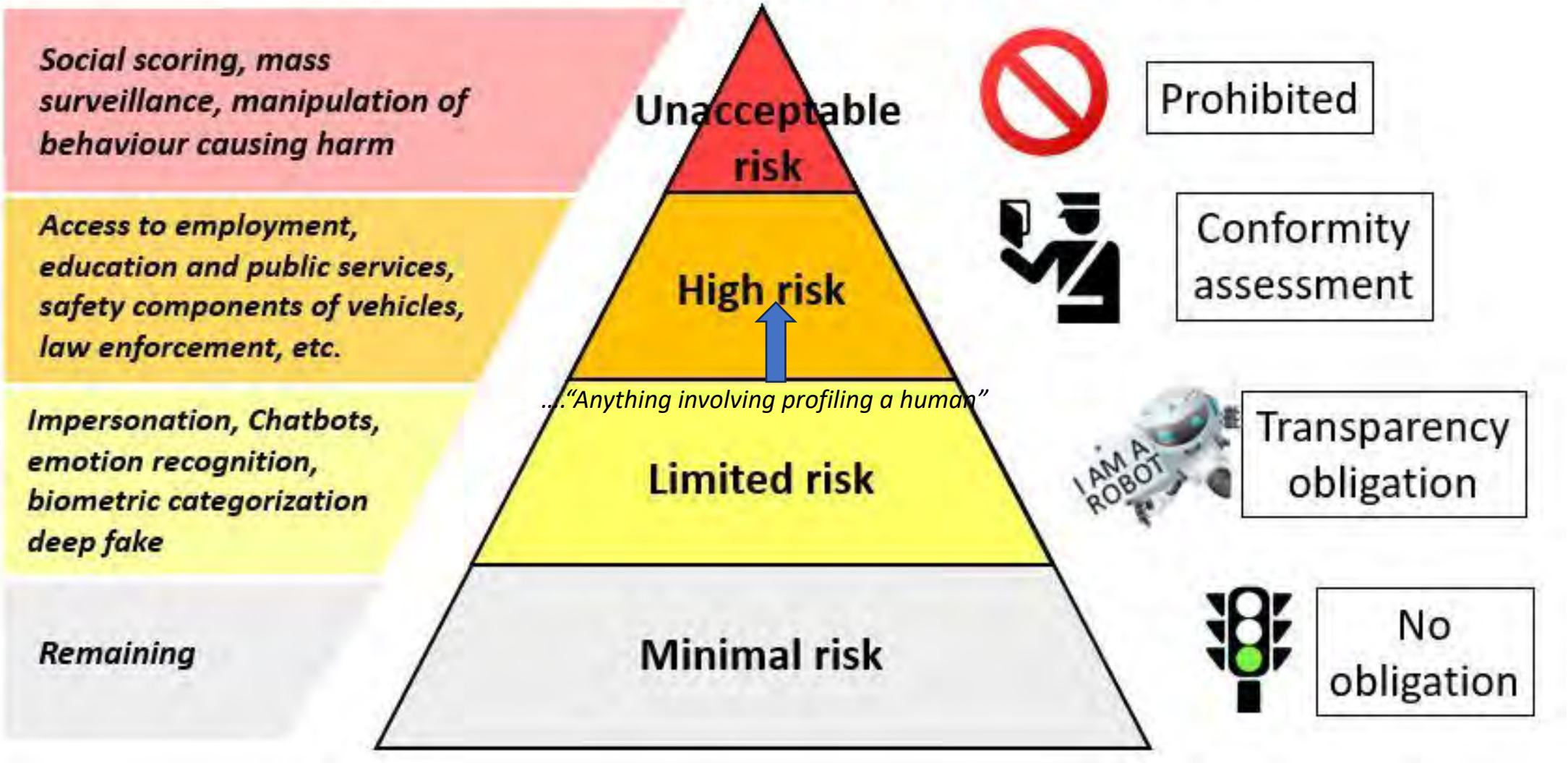


Image Source: Grabowicz, Perello, and Zick (2023), “Towards an AI Accountability Policy”

EU Artificial Intelligence Act: Risk levels

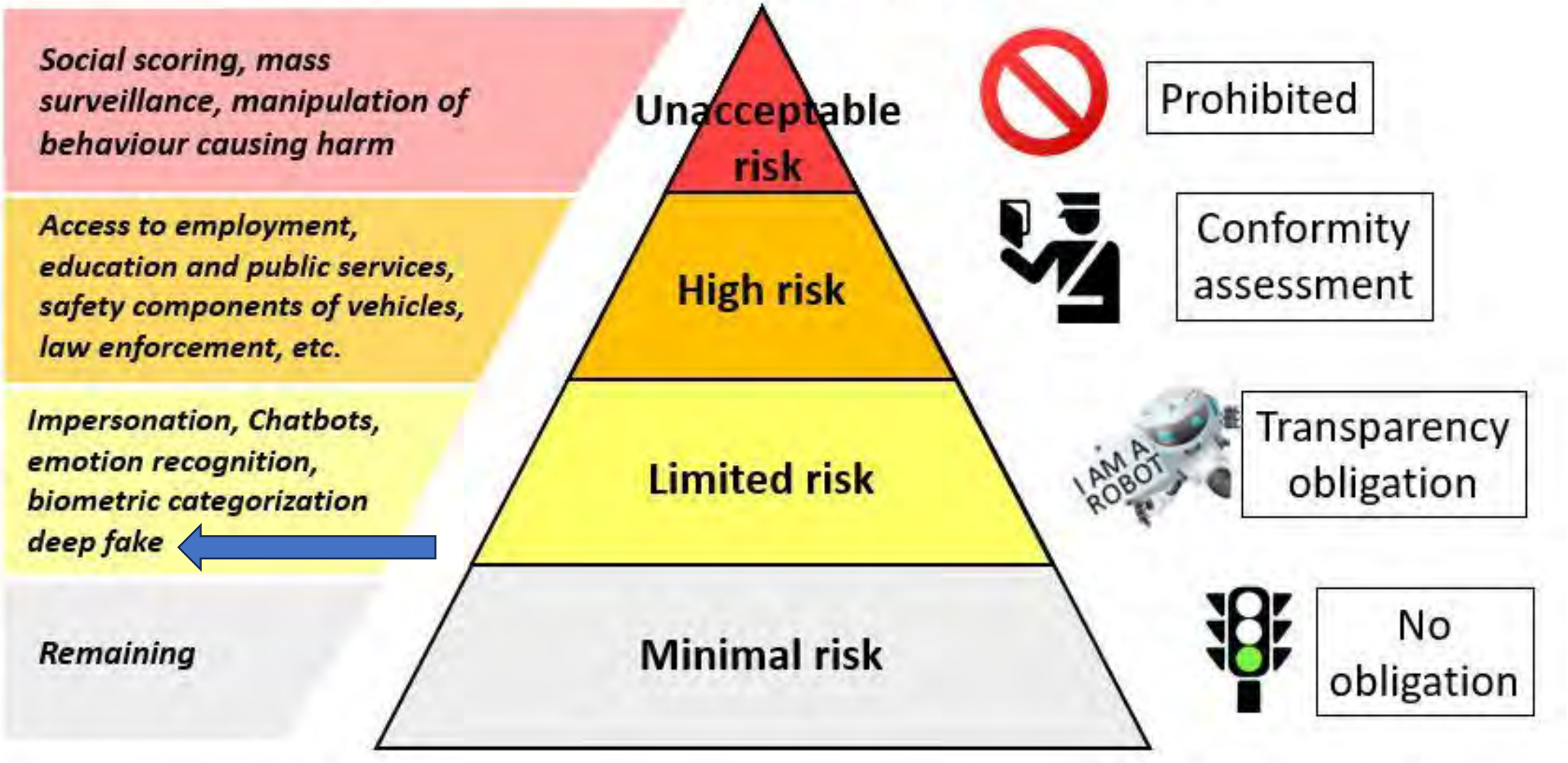


Image Source: Grabowicz, Perello, and Zick (2023), "Towards an AI Accountability Policy"

BHConsulting
Cybersecurity & Data Protection

Gemini

NB: 3 QUESTIONS THE BOARD SHOULD BE ASKING NOW:
1)TRAINING? 2)POLICY AND GUARDRAILS? 3)LICENSES?

BHConsulting
Cybersecurity & Data Protection

Why do emerging technologies present such a risk to Cyber and Privacy ?


KITCHEN

Numerous applications draw beneficial/troubling inferences recently.

INFERENTIAL/DERIVED DATA	ORGANIZATION
Sexual orientation, race, political opinion, imminent suicide attempts.	Facebook/Meta
Susceptibility to depression from users' posts/history.	Instagram and X
Links between physical behaviours and Parkinson's disease (e.g., tremors when using a mouse, repeat queries, scrolling velocity).	Microsoft
Scoring	Experian, Ebay, Uber
Judging citizens/organizations behaviour and trustworthiness.	China

Twitter taught Microsoft's AI chatbot t asshole in less than a day

by James Vincent | @jjvincent | Mar 24, 2016, 8:43am CDT

SHARE TWEET LINKEDIN

August 17

Kate Carruthers | UNSW

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

WILDEST DREAMS

SWIFTIES WANT A MASSIVE CRACKDOWN ON AI-GENERATED NUDES. THEY WON'T GET ONE

Sexually explicit images of the singer generated with AI software went viral on social media, and there's no good way to keep it from happening again

By MILES KLEE

JANUARY 25, 2024

ARTIFICIAL INTELLIGENCE

Fake News In Court: Attorney Sanctioned for Citing Fictitious Case Law Generated by AI

BHConsulting
Cybersecurity & Data Protection

How Should Boards Approach These Risks?

“Emerging tech has enabled the growth of new competitors, rapid-fire funding cycles, fluidity of technology, digital experiences demanded by customers, and the rise of non-traditional risks”.
McKinsey & Co.

McKinsey advocate 4 ways a board of directors deal with challenges associated with emerging tech & view themselves as catalysts for digital/cybersecurity transformation efforts :

1. Close the insights gap.
2. Understand how digital can upend business models.
3. Engage more frequently and deeply on strategy and risk.
4. Fine-tune the onboarding & fit of digital/cybersecurity directors.

BHConsulting
Cybersecurity & Data Protection

How Should Boards Approach These Risks?

5 Common Themes:

Accountability in Governance

✅ **Board-Level Responsibility** – Directors must ensure compliance and integrate cybersecurity, AI ethics, and data protection into business strategy.

✅ **Appoint Compliance Officers** – Assign a CISO for NIS2/CRA, an AI Compliance Officer for AI Act, and a DPO for GDPR (if required).

✅ **Risk-Based Approach** – Identify, assess, and manage risks related to cybersecurity, AI, and personal data.

✅ **Develop & Enforce Policies** – Implement and regularly update Cybersecurity Policies (NIS2/CRA), AI Governance Policies (AI Act), and Data Protection Policies (GDPR).

✅ **Conduct Risk Assessments** – Perform periodic cyber risk assessments (NIS/CRA), AI risk evaluations (AI Act), and DPIAs(GDPR).

✅ **Continuous Monitoring** – Implement monitoring mechanisms to detect cybersecurity threats, AI biases, and data privacy risks.

- ✅ **Timely Incident Reporting**

Ensure prompt reporting of cyber incidents (NIS2/CRA: can be 24 hours), AI-related failures (AI Act), and data breaches (GDPR: 72 hours).

✅ **Incident Response Plan**

Establish a clear response strategy for cybersecurity breaches, AI failures, and data leaks.

✅ **Crisis Management Training**

Train leadership and employees on how to handle security breaches, AI failures, and privacy violations.

✅ **Audit & Documentation** – Maintain proper records of cybersecurity controls (NIS2/CRA), AI decision-making (AI Act), and personal data processing (GDPR).

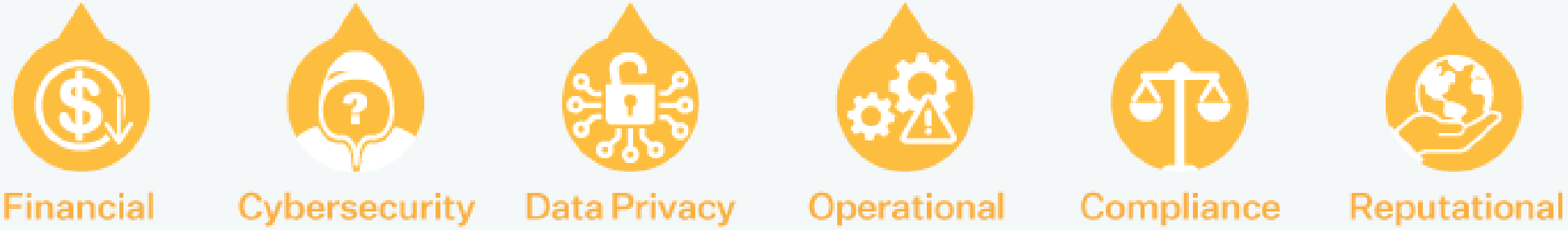
Compliance Audits – Internal audits to avoid penalties/regulatory scrutiny.

✅ **Explainability & Transparency** – Ensure AI models are explainable and compliant with data protection laws.

✅ **Ethical Decision-Making** – Establish processes to reduce biases in AI models, protect data privacy, and strengthen cybersecurity.

Third-Party Risk Assessment

The process used by companies to evaluate the risks they may encounter when working a third party, such as a vendor, supplier, contractor, or other business partner.



✅ **Regular Training Programs** – Train employees on cyber threats (NIS2/CRA), AI ethics (AI Act), and data protection (GDPR). Literacy vs Training?

✅ **Third-Party Risk Management** – Ensure suppliers and vendors comply with cybersecurity (NIS2/CRA), AI fairness (AI Act), and data protection (GDPR). Vendor Assessments.

✅ **Contract Reviews** – Include security, AI governance, and data protection clauses in vendor agreements (DPAs).

VALERIE.LYONS@BHCONSULTING.IE
Mobile: 00353851725370
www.linkedin.com/in/valerielyons-privsec

BHConsulting
Cybersecurity & Data Protection

Institute of Directors Ireland

Digital Governance: AI, Cybersecurity, and Privacy

with Dr. Valerie Lyons, Company Director, and Chief Operating Officer, BH Consulting

20th March 2025