Organized by

AUSCHAM VIETNAM

In Collaboration with

VIAC
VIETNAM INTERNATIONAL ARBITRATION CENTRE

Powered by

enablecode

ASIA LEGAL
BUSINESS LAW FIRM

QBE

EVENT MATERIALS

# WEBINAR

# AI, DIGITAL TRANSFORMATION AND CYBER RESILIENCE: WHAT BUSINESSES IN VIETNAM SHOULD PREPARE FOR?

## [VIAC x AUSCHAM WEBINAR SERIES 2026]

# Topic 03 – "AI, Digital Transformation and Cyber Resilience: What Businesses in Vietnam Should Prepare For?"

### INTRODUCTION

As Vietnam's business landscape rapidly evolves in the age of artificial intelligence and digital transformation, companies are facing unprecedented opportunities alongside growing cybersecurity risks. This webinar, **"AI, Digital Transformation and Cyber Resilience: What Businesses in Vietnam Should Prepare For?"**, will provide practical insights into how businesses can harness emerging technologies while strengthening their resilience against evolving cyber threats.

The session will bring together technology experts, digital transformation leaders, and cybersecurity practitioners to discuss the opportunities and challenges AI presents for businesses in Vietnam, the key digital transformation trends shaping industries, and the cyber resilience strategies organizations should adopt to stay secure and competitive.

**Key topics include:**

- 🔷 **AI and Digital Transformation Trends** – Explore how AI is reshaping business operations, decision-making, customer engagement, and productivity across industries in Vietnam.
- 🔷 **Emerging Cybersecurity Risks in the AI Era** – Understand the evolving threat landscape, including AI-powered cyberattacks, data breaches, ransomware, and other digital vulnerabilities businesses must prepare for.
- 🔷 **Building Cyber Resilience** – Learn practical strategies to strengthen cyber preparedness, improve incident response, and ensure business continuity in an increasingly digital environment.

This session is ideal for AusCham members, business leaders, technology professionals, risk managers, and companies seeking to accelerate digital transformation while safeguarding their operations against cyber threats.

### GENERAL INFORMATION

**Time:** 09:30 AM – 11:30 AM (GMT+7), Thursday, 23 July 2026

**Format**: Virtual via Zoom (VIAC)

**Language**: English

**Tickets**: FOC for All

**AGENDA**

| Timeframe | Content |
|---|---|
| 9.15 – 9.30 AM | Welcoming |
| 9.30 – 9.40 AM | **Opening Remarks and Introduction**<br><br>Representative from the Australian Chamber of Commerce in Vietnam (AusCham) |
| 9.40 – 10.10 AM | **Session 1: AI and Digital Transformation in Vietnam – Legal and Regulatory Landscape**<br><br>**Mr. Colin Blackwell** – CEO, Enablecode / Chairman, Hyperion Fintech AG<br><br>- AI adoption trends in Vietnam<br>- Key regulations affecting AI, data, and digital operations<br>- Personal data protection and compliance obligations<br>- Emerging governance around AI accountability and responsible use |
| 10.10 – 10.40 AM | **Session 2: Cyber Risks in the AI Era – Emerging Threats for Businesses – Risk Mitigation and Response Strategies for Businesses**<br><br>**Mr. Sam Russell-Vick** – Regional Cyber Lead, QBE Asia<br><br>- How AI changes the cyber threat landscape<br>- New attack vectors: phishing, deepfakes, ransomware, insider risks<br>- Real business impacts: financial loss, operational disruption, reputational damage<br>- Common gaps in corporate cyber preparedness<br>- Role of cyber insurance in risk transfer |
| 10.40 – 11.20 AM | **Session 3: When Things Go Wrong – Disputes in the Digital Economy**<br><br>**Mr. Luu Xuan Vinh** – Founder & Managing Partner, Asia Legal, FCIArb, FSIArb, FACICA<br><br>- Common disputes involving AI and digital transformation<br>- Cyber-attacks as a way to escape from contractual obligations?<br>- Electronic evidence and e-discovery: From data privacy to evidentiary disclosure<br><br>- Why arbitration for tech disputes? |
| 11.20 – 11.30 AM | **Q&A**<br><br>Moderated by: **Mr. Luu Xuan Vinh** – Founder & Managing Partner, Asia Legal, FCIArb, FSIArb, FACICA |
| 11.30 AM | **Closing** |

Organized by AUSCHAM VIETNAM

In Collaboration with VIAC

VIAC x AUSCHAM | 23 JULY 2026

# AI & DIGITAL TRANSFORMATION IN VIETNAM

## REGULATION, REALITY & RESPONSIBILITY

**COLIN BLACKWELL**

CEO, Enablecode | Chairman, Hyperion Fintech AG

# AI adoption is cultural as much as technological

Global Cultural Trajectories of AI Adoption

**INNOVATORS**

Move fast, regulate later, high risk tolerance

US, China

**TRUST-FIRST ECONOMIES**

Governance frameworks before scale deployment

EU, Australia, Canada

**HESITANT ECONOMIES**

Interested but cautious, limited institutional readiness

Many emerging markets

> *Vietnam is fascinating because all three models exist simultaneously inside one country.*

# AI is not creating the gap — it is amplifying it

## Vietnam's productivity divide is accelerating

**Vietnam is already a two-speed economy.**
AI is widening the existing productivity divide.

**Vietnam's 3-tier AI landscape:**

1. **Global-level capability:** FDI tech companies, leading Vietnamese tech firms
2. **Transitional organizations:** Actively exploring AI but lacking operational frameworks
3. **Slow adoption sectors:** Limited awareness, minimal digital infrastructure

**Strategic insight:**
Vietnam becomes a developed economy when the broader workforce closes the productivity gap.

# UP TO 4x

**Foreign firms' digital-sector output advantage can be up to four times greater.**

*The gap varies by sector and measure. The strategic point does not.*


**AI WILL MAKE THIS WORSE - UNLESS DOMESTIC CAPABILITY CATCHES UP.**

Source: OECD, FDI Qualities Review of Viet Nam (2026), Section 3.2.3 and Figure 3.5.

AI IN BUSINESS – SIGNAL OR NOISE?

# Vietnam should not be viewed as a traditional outsourcing market

## Traditional BPO centers are becoming obsolete

**THE SHIFT**
Traditional BPO centers focused on low cognitive tasks are becoming obsolete because AI has already replaced those functions.

**THE FUTURE MODEL**
Instead of thousands of people in a traditional BPO center, organizations need a few highly skilled AI specialists managing complex workflows and AI agents.

**VIETNAM'S ADVANTAGE**
- Adaptive talent pool with strong technical aptitude
- Deep engineering capability
- Fast-moving workforce comfortable with rapid technology change

FROM MASSIVE TO MANY

TO A FEW WHO LEAD


| STRATEGIC REFRAMING | | |
|---|---|---|
| Thousands of low-cognitive BPO workers | → | A few elite AI specialists managing workflows |
| Outsourcing destination | → | AI co-development ecosystem |
| Cost arbitrage play | → | Innovation partnership model |

# AI adoption and use advances faster than both regulation and governance

## The operational reality outpaces the frameworks

### OPERATIONAL REALITY

Shadow AI usage is widespread. Organizations are deploying AI for productivity faster than formal policies can be drafted.

### THE CORE ISSUE

Technology is changing much faster than legislative frameworks can be researched, drafted, consulted on and implemented.

### THE CHALLENGE: MANAGED TRANSFORMATION

Building capability for both innovation and governance simultaneously.

The future belongs to organizations that can **innovate responsibly—faster.**

BOARDROOM REALITY

## The law is not the slow part. Your company is.

| | |
|---|---|
| **OWNER** | Who is accountable? |
| **INVENTORY** | What AI is actually in use? |
| **APPROVAL** | What can be deployed, by whom? |
| **MONITOR** | What evidence is kept? |
| **RESPOND** | What happens when it fails? |

***A policy without an owner is just a PDF.***

# The rules changed on 1 July. Most companies did not.

**Vietnam's Cybersecurity and Digital Transformation laws are now in force.**

ALREADY LIVE

| | |
|---|---|
| **1 JUL 2025** | Data Law |
| **1 JAN 2026** | Personal Data Protection Law + Decree 356 |
| **1 MAR 2026** | Artificial Intelligence Law |

**1 JUL 2026** **Cybersecurity Law | Digital Transformation Law**

***The operating gap just became a compliance gap.***

***The question is no longer whether your business is using AI. It is whether you can explain what it is doing.***


Sources: Law 116/2025/QH15 and Law 148/2025/QH15; both effective 1 July 2026.

# Vietnam did not wait for the rest of the world.

**The ambition was never the problem. Execution is.**

**2026**

**THE RULES ARE LIVE**

THE REGULATORY STACK NOW IN FORCE

| | | | |
|---|---|---|---|
| 1 | 1 JUL 2025 | **Data Law 60/2024/QH15** | Data governance and protection |
| 2 | 1 JAN 2026 | **PDP Law 91/2025/QH15** | Personal data duties + Decree 356 |
| 3 | 1 MAR 2026 | **AI Law 134/2025/QH15** | Risk, transparency and accountability |
| 4 | 1 JUL 2026 | **Cybersecurity Law 116/2025/QH15** | Unified cybersecurity obligations |
| 5 | 1 JUL 2026 | **Digital Transformation Law 148/2025/QH15** | Digital operations and transformation |

**FIVE LAWS. ONE OPERATING MODEL. NO PLACE LEFT TO HIDE.**


Sources: official Government legal database, vanban.chinhphu.vn. Business overview only; confirm application with Vietnamese counsel.

# The AI Law does not regulate intelligence. It regulates responsibility.

**Three verbs describe the job.**

## 1 CLASSIFY

High, medium or low risk. Medium and high-risk systems require formal classification and notification.

## 2 DISCLOSE

Tell people when they are interacting with AI. Label synthetic audio, images and video where required.

## 3 CONTROL

Maintain human oversight, safety, records, incident handling and the ability to explain what happened.

**EXISTING SYSTEMS DO NOT GET A FREE PASS**

**12 MONTHS**

Most existing AI systems

**18 MONTHS**

Healthcare, education and finance

**PROVIDER / DEPLOYER / USER**

Different roles. Different duties. Know which one you are.

Source: Law 134/2025/QH15, Arts. 9-15 and 34-35. Effective 1 March 2026.

# Your AI strategy is already a data strategy - whether you admit it or not.

**Personal data is where interesting experiments become real obligations.**

1. **Know what enters the model**
   Map personal data, prompts, outputs, logs and training data.
2. **Document the purpose**
   Record access, retention, vendors and the legal basis for processing.
3. **Assess the impact**
   Complete processing and cross-border transfer assessments where required.
4. **Put somebody in charge**
   Assign accountable personal-data protection personnel and escalation routes.
5. **Prepare for failure**
   Build an incident process before a breach, complaint or regulator request.

**60**
**DAYS**
**The clock starts when processing starts.**

**DECREE 13 IS NOT THE CURRENT ANCHOR.**
**The 2025 Personal Data Protection Law + Decree 356 are.**

Source: Law 91/2025/QH15, Arts. 21-22; Decree 356/2025/ND-CP. Business overview only.

# The next 90 days: find it, classify it, control it.

**Do not start with a committee. Start with evidence.**

**90 DAYS**
**NO COMMITTEE REQUIRED**

**0-30 FIND IT**
Inventory AI systems, shadow use, data flows and vendors.

**31-60 CLASSIFY IT**
Determine risk, legal role, impact assessments and human decision points.

**61-90 CONTROL IT**
Set approval, contracts, logging, incident response and workforce training.

***If nobody owns the system, everybody owns the failure.***

**EVIDENCE FIRST.**

# AI is not ultimately about technology or law. It is a workforce transformation.


**Technology and compliance are necessary. Neither is sufficient.**

- **Leadership** — willingness to embrace uncertainty
- **Workforce capability** — continuous upskilling at scale
- **Adaptability** — organizational agility and learning speed
- **Culture** — permission to experiment and fail
- **Speed of learning** — closing the gap between knowledge and action

***The organisations that succeed with AI will not be those with the best technology or the biggest compliance file — but those that adapt their people and operating models the fastest.***

QBE Insurance

# The Role of Cyber Insurance in an Emerging Threat Landscape

Date: 23rd July 2026

Sam Russell-Vick – Regional Cyber Lead, Asia

## Agenda

1 Emerging Cyber Threat Landscape

2 QBE Cyber Coverage

3 QBE Claim Case Studies



QBE

QBE Insurance

# Emerging Cyber Threat Landscape

## Key Cyber Claim Trend Triggers

### Ransomware

Ransomware remains the defining threat to almost all sectors

### Extortion

The tempo of extortion attacks is at an all time high by the end of 2025

### Social Engineering

Social engineering, perimeter exploitation and identity theft are key enablers

### Supply Chain

Supply chain attacks are another key risk area for many organisations


### Payment

Percentage of extortion cases resulting in payment increased

### State Sponsored

State sponsored activity aligning heavily with national priorities

### Long Term Access

Long-term access and pre-positioning as key strategic priority

### AI Usage

Significant increase in use of AI to enhance cyber capabilities



QBE

# GenAI: A New Weapon for Threat Actors

| | |
|---|---|
| IBM Phishing Study | IBM X-Force conducted a controlled study pitting AI (via ChatGPT) against experienced human social engineers in crafting phishing emails. The AI produced highly convincing, targeted phishing messages in just 5 minutes using five prompts—compared to the 16 hours the human experts took—and, alarmingly, its effectiveness was nearly equivalent to that of the humans*. |

QBE Report: Reimagining Commercial Espionage and Fraud in the Era of Agentic AI

**Adversary use of Gen AI spans three primary sectors:**

### Social Engineering

- **Identity Generation**
- Social Engineering Optimization: *With the assistance of advanced AI tools such as ChatGPT, an attacker can generate a phishing login page in under ten minutes.*

### Technical Operations

- **Vulnerability exploitation**
- Malware advancement; *Prompt flux is an AI-driven malware that leverages LLM APIs (Gemini) to dynamically rewrite itself, generate malicious code and evade detection.*

### Information Operations

- **Multilingual adaptation**
- Disinformation content: *In **2024**, **Arup**, an engineering firm based in the Hong Kong, fell victim to a deepfake attack, which led to a loss of **$25 million.***



QBE

# Cyber Threat Analysis

## Legal & Professional Services (LPS) Sectors

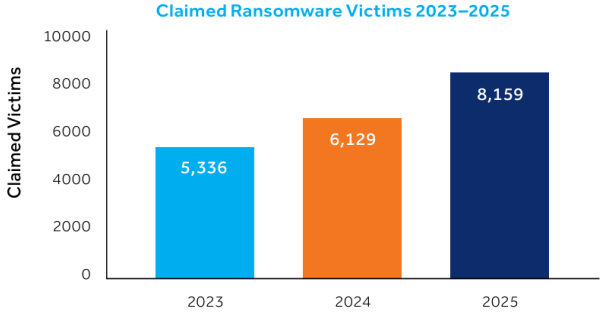
***QBE Report:** Cyber Threats Legal and Professional Services Sector*

**Executive Summary**

- The **cyber threat** to the LPS sector has remained a key risk as we progress through 2026.
- It remains one of the **most targeted sectors** by highly active and sophisticated ransomware actors, as well as some state sponsored groups.
- The legal and professional services sector should remain aware of broader threat trends including how **social engineering (AI Enhanced)** and the exploitation of **critical vulnerabilities** has increasingly enabled threat actors to launch highly impactful attacks in 2025.
- While **ransom payment** rates have generally decreased, the legal sector remains one of the most **heavily targeted sectors** by ransomware actors.
- So far in 2026, the sector remains one of the most targeted globally, with high numbers of known **victims across** the US, UK, Australia and **Asia**.

**Ransomware & Extortion**

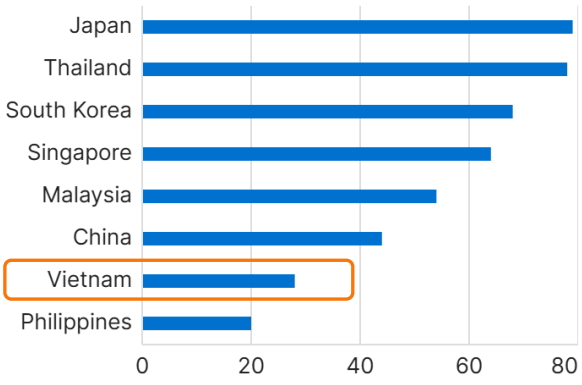
- **New groups have emerged**, existing groups have ramped up their operations, while others have disappeared.
- What is clear is that **ransomware** and **data extortion** continues to be the most significant threat to almost every industry vertical, especially the **LPS sector**.



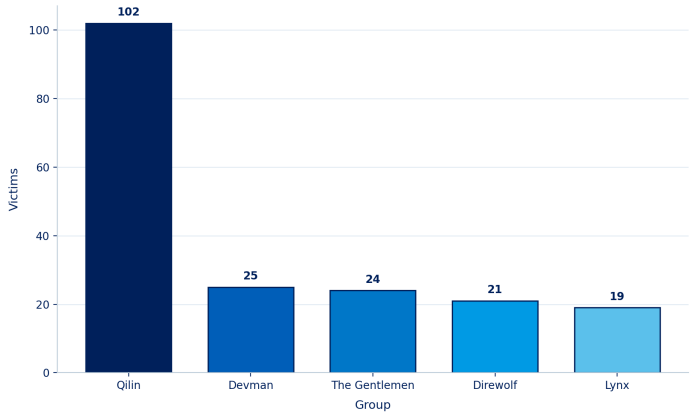



QBE

# Asia Threat Landscape




*Number of publicly known ransomware victims between Jan 2025 – Jan 2026*



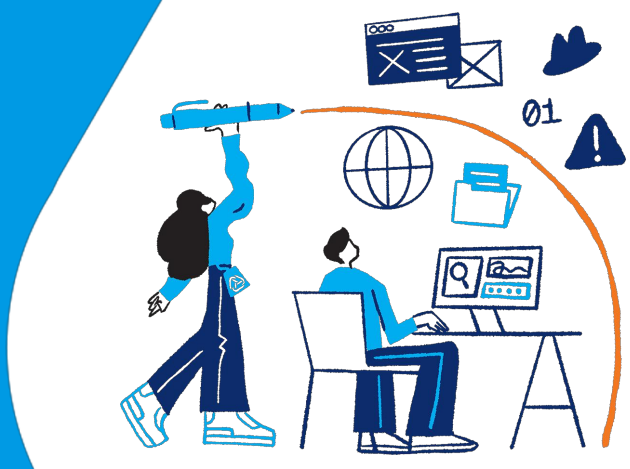

*Top ransomware groups in Asia: Number of victims by group between Jan 2025 – Jan 2026*



QBE

QBE Insurance

# QBE Cyber Coverage



# QBE Cyber Coverage

Topics to cover:

1. Third Party Liability Risk
2. First Party Risk
3. Business Interruption & Reputation Risk




QBE

QBE Insurance

# Third Party Liability

# Third Party Liability Risk

## What is the current situation?

- Companies are consuming data like never before, "Data is the new oil" [1]
- Regulators around the world have varying laws and regulations, including regulations around the development and use of AI.
- The Data Privacy Laws are changing and becoming more onerous and evolving to address AI related exposures.

[1]



# Third Party Liability Risk

## What is the problem?

- Increasing public concern for data privacy around the world. I.e. Data privacy driven lawsuits and class actions are on the rise. [1]
- Regulators are getting tougher. E.g. Fines & Penalties are increasing under the new **Vietnam PDPL** regulation (Up to 5% annual revenue fine). [2]
- Operational and real-world implications for businesses:
  - **Vietnam PDPL 2025**, effective 1 January 2026, notification of data breach related incidents within **72 hours** [3]
  - **The Cyberspace Administration of China** ("**CAC**"): new stricter and **4-hour** data breach reporting requirements for certain incidents [4]
  - **Singapore PDPA** mandates you must notify within **3 business days.** [5]


[6]

# Third Party Liability Risk

What is the solution?

## Cyber Insurance!



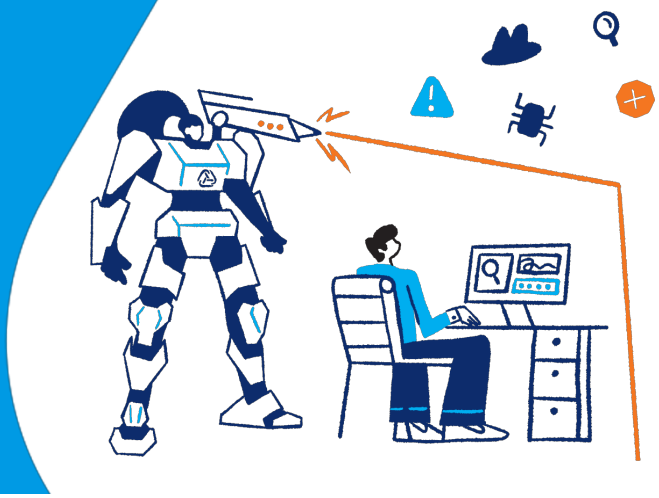
# Third Party Liability Risk

### QCyberProtect Coverage

- Worldwide protection against civil data privacy damages and disputes.
- Worldwide protection against data privacy related regulatory insurable fines and penalties.
- Worldwide protection against regulator cyber security acts obligations.
- Legal counsel support and assistance with managing regulatory data breach notification requirements.
- PCI-DSS liability.
- Media content liability.
- AI regulations concerning the development and use of AI.

QBE Insurance

# First Party Risk



## First Party Risk

### What is the current situation?

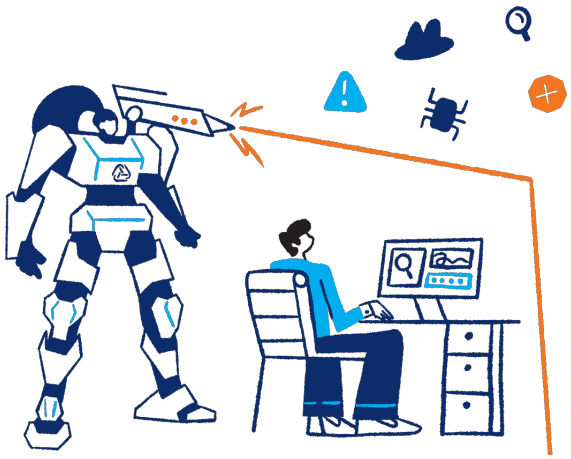
- We're more reliant on Information Technology than ever before.
- Nearly every company uses technology in one shape or form.
- Technology has allowed us to be more productive and efficient.

[1]

# First Party Risk

## QCyberProtect Coverage

- Access to 24/7 specialist incident response services.
- Digital forensic investigation and response.
- Crisis communication and public relations.
- Ransomware negotiations and legal payments.
- Third-party system hosting while your systems are being brought back online.
- Hardware replacement costs.
- Large Language Model (LLM) jacking costs.
- Cyber crime coverage around fund transfers and social engineering losses.





QBE Insurance

# Business Interruption & Reputation Risk

# Business Interruption & Reputation Risk

## What is the current situation?

- Technology allows our businesses to operate around the clock.
- We can leverage technology to become more efficient.
- It enables us to offer a better service, and customs are drawn to that.

[1]

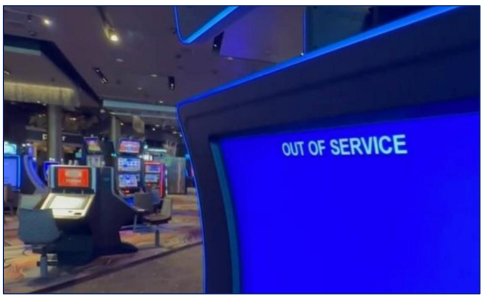


QBE

# Business Interruption & Reputation Risk

## What is the problem?

- Financial Loss. E.g. Loss of Income.
- Inability to function and loss of quality control. E.g. Errors in production.
- Consequential Reputational Loss. Ie. Loss of customers.




[1]



QBE

# Business Interruption & Reputation Risk

What is the solution?

## Cyber Insurance!



QBE

# Business Interruption & Reputation Risk

### QCyberProtect Coverage

- Loss of net profit (before tax) arising from a broad range of cyber scenarios:
  - Cyber attacks.
  - Non-malicious system failures.
  - Voluntary shutdowns.
  - IT-Services provider outages.
  - Non-IT services providers cyber incidents (supply chain risk).
- Loss adjusting quantification costs.
- Loss of net profit (before tax) that the insured would have earned if not for the adverse publicity.




QBE

QBE Insurance

# QBE Claim Case Study

## Claims expertise that restores control fast

**Case Study:** Smart containment and cost-efficient recovery
**Client:** Law Firm - Asia
**Industry:** Legal Services
**Challenge:** Ransomware attack with confirmed data exfiltration and multi-system encryption

### The Incident

A law firm in Asia experienced a sophisticated ransomware attack after a threat actor gained access via a compromised VPN.

Once inside the network, the attacker escalated privileges, encrypted virtual machines, and exfiltrated sensitive data, resulting in system lockout and a **ransom demand** of USD 400k.

### The QBE difference

QBE Claims immediately activated incident response and coordinated a full forensic, legal, and containment strategy.

Working closely with specialist partners:

- Deployed enterprise-grade endpoint monitoring to identify and isolate the threat
- Removed threat actors and secured affected systems
- QBE's panel specialists facilitated and managed the ransom payment down to USD 100k
- Supported regulatory notification requirements where needed

### The Outcome

- Insured **restored** operations safely after containment and isolation of encrypted systems
- Regulatory response was **supported** through forensic analysis and documented findings
- **Cost-effectively** managed through ensuring all activities fell within covered sections
- **Coordinated** with the client to mitigate reputational and operational impact

QBE

# AI, Digital Transformation and Cyber Resilience: What Businesses in Vietnam Should Prepare For?

## Session 3: When Things Go Wrong – Disputes in the Digital Economy

ASIA LEGAL_Dữ Liệu Cá Nhân
Zalo community

Scan this QR code with Zalo to join


**PRESENTED BY:**

### LL.M. / Attorney-at-Law LUU XUAN VINH

- **Founding & Managing Partner |** Asia Legal
- **Fellow |** CIArb, SIArb, ACICA
- **Arbitrator |** VIAC (Vietnam), DIAC (Dubai), ACICA (Australia), SHAC (PRC)
- **Head of Legal |** Swiss-Vietnam Economic Forum (SVEF)
- **Head of International Relations |** Vietnam M&A Association (VMAA)
- **Deputy Head of Legal Committee |** Vietnam Association of Foreign Invested Enterprises (VAFIE)
- **Law Lecturer |** Judicial Academy of Vietnam

M: 091 626 3656 E: vinh.luu@asialegal.vn W: asialegal.vn | dataprivacy.vn

# CONTENTS



# PART 01

# COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION

**US AI Disputes Tracker (Fisher Phillips LLP)** - tracks U.S. disputes involving AI across all 50 states, classified by sector and area of law.
Coverage: 25 February 2021 – 22 June 2026.
AI Litigation Tracker

| Metrix | Result |
|---|---|
| Total cases recorded | 245 cases |
| Top sector - Technology | 146 cases |
| Top sector - Real estate | 22 cases |
| Top area of law - Artificial intelligence | 88 cases |
| Area of law - Privacy | 78 cases |
| Area of law - ALPR (automated license plate recognition) | 34 cases |

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

**Global Disputes Forecast 2025** - 44% of respondents flag AI-related disputes as a significant risk.
Baker McKenzie Annual Disputes Survey: Technology-Related Issues Top 2025 Disputes Risk

| Concern | Share of respondents |
|---|---|
| Data privacy & security | 60% |
| Ethical disputes | 59% |
| IP disputes (infringement risk in AI-generated output, third-party trademark / personality rights, ownership & protectability of AI-assisted content) | 55% |

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

**Reported AI incidents have risen sharply - staying under 100/year until 2022 and reaching 362 in 2025.**
Artificial Intelligence Index Report 2026

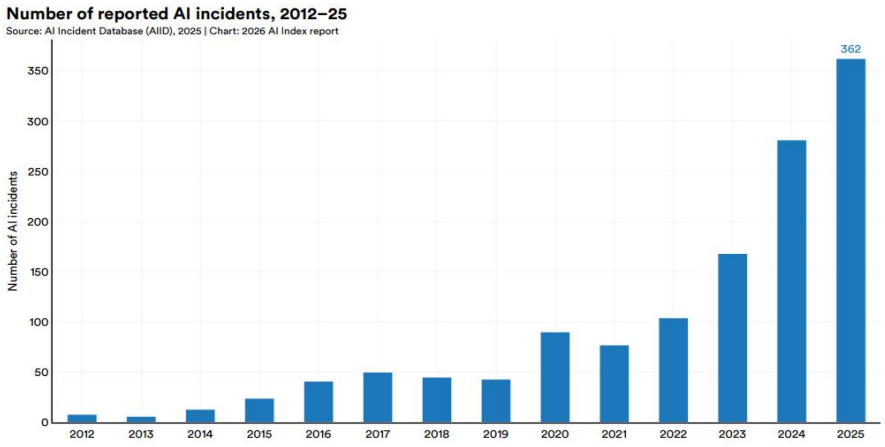



Figure 3.2.1[2]

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

01. Intellectual Property Disputes
02. Data Privacy & Security Disputes
03. Hallucination and Bias Disputes
04. Service Level Agreement and Smart Contract Disputes

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

### 01. Intellectual Property Disputes

**a) Input/Training Data:** AI developers routinely engage in the unauthorized mass extraction of data (web scraping) from the internet for the purpose of training machine learning models, in the absence of any express license or consent from the data rights holders.

**Case Study:** *The New York Times v. OpenAI and Microsoft*

**b) Output/AI-generated Content:** Who owns works generated by AI?

**Case Study:**

- *Li Yunkai (Beijing Internet Court, judgment of 17 November 2023;*
- *Thaler v. Perlmutter (United States Court of Appeals, No. 23-5233, decided 18 March 2025)*

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

### 02. Data Privacy & Security Disputes

**Insider Threats:** Employees inputting **proprietary source code** or **sensitive client data**—such as medical or financial records—into ChatGPT for analysis pose a significant risk.

**Case Study:**

- *Samsung Semiconductor (2023)*
- *Adobe data breach*

**Compliance Landscape in Vietnam:** Decree 356 has further tightened regulations governing **cross-border data transfer** and mandates **impact assessments** for **fully automated algorithmic decision-making systems**.

## COMMON DISPUTES INVOLVING AI AND DIGITAL TRANSFORMATION (Cont.)

### 03. Hallucination and Bias Disputes

**a) Financial Liability Arising from AI Misinformation;**

**Case Study:** *Moffatt vs Air Canada (February 2024)*

**b) Algorithmic Bias in Recruitment and Lending**

**Case Study:** *U.S. Equal Employment Opportunity Commission (EEOC) vs iTutorGroup (2023)*

### 04. Service Level Agreement and Smart Contract Disputes

**a) Breach of AI Service Level Agreements (SLAs);**

**b) Implementation Errors in Smart Contracts**

**Case Study**: *MD Anderson v. IBM Watson (2017)*

# PART 02

# CYBER-ATTACKS AS A WAY TO ESCAPE FROM CONTRACTUAL OBLIGATIONS

## CYBER-ATTACKS AS A WAY TO ESCAPE FROM CONTRACTUAL OBLIGATIONS

**Statistics on the losses incurred following cyber incidents: Cost of Data Breach Report 2025 (IBM)**
Global average cost of a data breach: USD 4.44 million.
Cost of a Data Breach Report 2025

Figure 2.
Measured in USD millions

| # | Country | | 2025 | 2024 |
|---|---|---|---|---|
| 1 | United States | ↑ | $10.22 | $9.36 |
| 2 | Middle East | ↓ | $7.29 | $8.75 |
| 3 | Benelux | ↑ | $6.24 | $5.90 |
| 4 | Canada | ↑ | $4.84 | $4.66 |
| 5 | United Kingdom | ↓ | $4.14 | $4.53 |
| 6 | Germany | ↓ | $4.03 | $5.31 |
| 9 | ASEAN | ↑ | $3.67 | $3.23 |
| 10 | Japan | ↓ | $3.65 | $4.19 |
| 11 | Italy | ↓ | $3.44 | $4.73 |
| 12 | South Korea | ↓ | $2.84 | $3.62 |
| 13 | Australia | ↓ | $2.55 | $2.78 |
| 14 | India | ↑ | $2.51 | $2.35 |

*Figure - Global average cost of a data breach*

## CYBER-ATTACKS AS A WAY TO ESCAPE FROM CONTRACTUAL OBLIGATIONS (Cont.)

***Statistics of Cyberattacks in Vietnam***
**Vietnam - National Cybersecurity Association (2025)**: data security is becoming a major challenge as Vietnam's digital transformation accelerates.
Over 50% of agencies and businesses hit by cyberattacks in 2025

| Metrix | Result |
|---|---|
| Cyberattacks on Vietnamese systems (2025) | ~552,000 (↓ 19.38% vs. 2024) |
| Organizations reporting actual damage (2025) | 52.30% (↑ 46.15% vs. 2024) |
| Top 5 attack types (2025) | DDoS, blacklinking, APTs, data theft, ransomware |

## CYBER-ATTACKS AS A WAY TO ESCAPE FROM CONTRACTUAL OBLIGATIONS (Cont.)

**1) Using Cyberattacks as a "Force Majeure" Shield**

When enterprises fall victim to **cyberattacks**—such as ransomware or DDoS—that result in **system outages**, **client data breaches**, or **delivery delays**, they frequently invoke **"Force Majeure"** clauses to evade liability for breaching **Service Level Agreements (SLAs)**. However, under contemporary legal frameworks (including the 2015 Civil Code of Vietnam), a standard cyberattack rarely satisfies the strict legal requirements to qualify as a ***Force Majeure*** **event**.

**2) Staged Cyberattacks**

This represents the **"dark side" of the digital economy**, particularly prevalent in the realms of **Blockchain, Smart Contracts,** and **Digital Assets**. Development teams may intentionally **embed vulnerabilities** within the **source code**, subsequently **feigning a cyberattack** to legitimize the **misappropriation** of millions of dollars from partners or investors.

**Case Studies:**

- *Paris Court of Appeal, Case No. 18/03616 (Judgment of 7 February 2020, France)*
- *NotPetya*
- *Heritage Valley Health Sys. v. Nuance Communs., Inc. (United States, 2020)*

## CYBER-ATTACKS AS A WAY TO ESCAPE FROM CONTRACTUAL OBLIGATIONS (Cont.)

### Force Majeure Test

| Force Majeure Criteria | Application to Cybersecurity Risks | Legal Findings |
|---|---|---|
| Objectivity (External occurrence) | Cyberattacks are perpetrated by third-party hackers. | **Satisfied** (provided that no insider involvement is proven). |
| Unforeseeability | Cyberattacks occur daily and constitute an inherent risk in the digital economy. | **Not satisfied.** Enterprises are expected to anticipate and mitigate such risks when operating digitally. |
| Irresistibility (Unavoidable despite all measures) | Were security patches updated? Are there independent backup systems? Was data encrypted to standard? | **Not satisfied.** Most breaches result from outdated security systems or human negligence |

# PART 03

# ELECTRONIC EVIDENCE AND E-DISCOVERY: FROM DATE PRIVACY TO EVIDENTIARY DISCLOSURE


## ELECTRONIC EVIDENCE AND E-DISCOVERY: FROM DATA PRIVACY TO EVIDENTIARY DISCLOSURE

### 1) The Core Paradox: Duty of Disclosure vs. Data Privacy

When commercial disputes arise, particularly in international arbitration centers (e.g., VIAC, SIAC, ICC), the principle of **"Transparency"** mandates that parties produce **all relevant evidence**. In the digital era, however, this clashes head-on with **the principle of "Data Privacy"**

| E-Discovery Principle | Data Privacy Principle | Legal Flashpoint |
|---|---|---|
| **Broad Collection:** Requirement to gather all emails, messages, and server data to locate evidence. | **Data Minimization:** Requirement to process data only to the extent necessary for the original purpose. | Excessive data collection constitutes a violation of the data minimization principle. |
| **Disclosure:** Production of evidence to Arbitrators, opposing counsel, and experts. | **Confidentiality & Access Restrictions:** Prohibition of third-party access to personal data without consent. | Unredacted production of evidence constitutes a data breach. |

## ELECTRONIC EVIDENCE AND E-DISCOVERY: FROM DATA PRIVACY TO EVIDENTIARY DISCLOSURE (Cont.)

### 2) E-Discovery in the AI Era: Using Technology to Address Technology

Historically, reviewing millions of documents to extract evidence was a month-long, multi-million dollar undertaking. Today, we utilize **Technology-Assisted Review (TAR)** to solve this:

**Predictive Coding:** Senior counsel merely needs to review and label a few hundred sample documents as "relevant" or "non-relevant." The Machine Learning (ML) model then learns the counsel's legal logic and automatically scans the remaining millions of documents with high percentage of **accuracy**.

**Sentiment & Network Analysis:** Modern E-discovery tools go beyond keyword searches. AI can map **"Relationship Networks"** (identifying who chats with whom late at night) and detect shifts in sentiment within **Slack/Teams messages** (from professional to panicked/evasive) to pinpoint the exact location of the **"Smoking Gun."**

## ELECTRONIC EVIDENCE AND E-DISCOVERY: FROM DATA PRIVACY TO EVIDENTIARY DISCLOSURE (Cont.)

### 3) The Legal Scenario in Vietnam: Cross-border E-Discovery & Decree 356/2025

When FDI companies or Vietnamese corporations participate in international arbitration (e.g., in Singapore), E-discovery processes often collide with severe domestic legal barriers.

**The Scenario:** A Ho Chi Minh City-based firm exports its entire accounting server and internal email database, compresses it into a Zip file, and transfers it via Cloud to an Arbitral Tribunal in Singapore as evidence.

**Legal Violations:** Under Decree 13/2023 and the newly enacted Decree 356/2025, this action constitutes "unauthorized cross-border transfer of personal data.“

**Consequences:** The enterprise may win the case in Australia, but upon returning to Vietnam, it will face astronomical fines and potential suspension of its data processing activities because it failed to file a **Data Protection Impact Assessment (DPIA)** with the Ministry of Public Security and failed to obtain necessary consent from the data subjects mentioned in those emails.

### Practical Scenario: Disputes arising from "Shadow IT" in Vietnam

**Context:** Many businesses in Vietnam bypass official channels, opting to conduct business and contract negotiations via employees' personal Zalo, Viber, or Telegram accounts—a phenomenon known as **"Shadow IT"**

**The Dispute:** Upon discovering fraud or partner misconduct, the company demands that an employee surrender their personal phone to extract Zalo messages as evidence for litigation. The employee refuses, citing the constitutional right to privacy of correspondence and the Personal Data Protection Law.

**Deadlock:** The company cannot introduce these messages before a court or tribunal without proving the legality of the collection. Furthermore, they risk a counter-suit from the employee for privacy infringement.

# PART 04

## WHY ARBITRATION FOR TECH DISPUTES?

## WHY ARBITRATION FOR TECH DISPUTES?

**01. The Right to Appoint "Tech-Savvy Arbitrators“**

**02. Absolute Confidentiality**

**03. Procedural Flexibility & E-Discovery**

**04. Global Enforceability**

## WHY ARBITRATION FOR TECH DISPUTES? (Cont.)

### 01. The Right to Appoint "Tech-Savvy Arbitrators”

**The Judicial Challenge:** lack the capacity to interpret source code, comprehend the "black box" nature of AI algorithms, or decipher the mechanics of Smart Contracts.

**The Arbitral Advantage:** Autonomy to select your arbitrator who possesses not only legal acumen but also an engineering or technological background.

### 02. Absolute Confidentiality (The Lifeblood of Tech)

**The Judicial Challenge:** Court proceedings are typically public. Litigation filings and evidence—including proprietary source code, business strategies, and client lists—risk being exposed to the press or competitors.

**The Arbitral Advantage:** Confidentiality is the default. The entire proceeding, including E-discovery data and the final award, remains private.

## WHY ARBITRATION FOR TECH DISPUTES? (Cont.)

### 03. Procedural Flexibility & E-Discovery

**The Judicial Challenge:** Court procedures are often rigid and struggle to keep pace with technological advancements. Traditional E-discovery protocols are frequently sluggish and lack the sophisticated digital tools required for complex tech disputes.

**The Arbitral Advantage:** The Arbitral Tribunal can establish tailored "Procedural Orders" for the case. You can reach an agreement on the data extraction methodology, the use of AI for Technology-Assisted Review (TAR), and the verification of forensic digital evidence (such as log files), ensuring the most efficient process possible without being constrained by outdated civil procedure codes.

### 04. Global Enforceability

**The Judicial Challenge:** A national court judgment is notoriously difficult to recognize and enforce in other jurisdictions, often requiring a complex, multi-layered validation process.

**The Arbitral Advantage:** Under the 1958 New York Convention, arbitral awards are recognized and enforceable in over 170 countries. For cross-border technology contracts (e.g., a Vietnamese company hiring developers in India and selling solutions to a Japanese client), this is the "golden key" to securing your rights if a partner defaults or absconds.

## VIAC MODEL ARBITRATION CLAUSE

*“Any dispute arising out of or in relation with this contract shall be resolved by arbitration at the Vietnam International Arbitration Centre (VIAC) in accordance with its Rules of Arbitration”.*

### Parties may wish to consider adding:

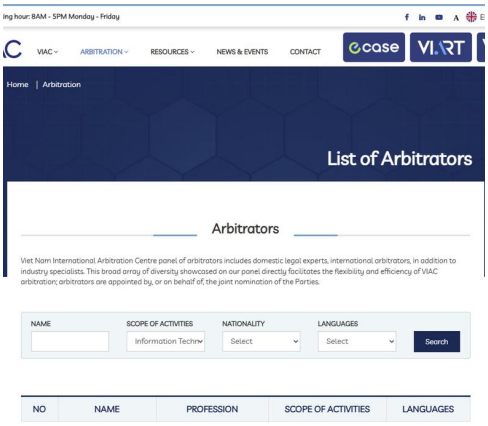
(a) the number of arbitrators shall be [one or three].
(b) the place of arbitration shall be [city and/or country].
(c) the governing law of the contract [is/shall be] the substantive law of [ ].*
(d) the language to be used in the arbitral proceedings shall be [ ].**

*Note:*
** For disputes which involve a foreign element.*
*** For disputes which involve a foreign element or disputes in which at least one party is an enterprise with foreign investment capital.*

Link: Model Arbitration Clause

# VIAC LIST OF ARBITRATORS WITH EXPERTISE IN TECHNOLOGY

## Step 1: In the List of Arbitrators, select the Scope of Activities: Information Technology




## Step 2: Select the Arbitrator from the List

| NO | NAME | PROFESSION | SCOPE OF ACTIVITIES | LANGUAGES |
|---|---|---|---|---|
| 1 | COLIN ONG | Senior Partner at Dr. Colin Ong Legal Services | Commerce, Banking & Finance, Construction, Energy, Information Technology | English, Chinese, Malay |
| 2 | MICHAEL LEE K. | Partner \| Dilinh Legal | Mergers and Acquisitions, Commerce, Real Estate, Construction, Information Technology | Vietnamese, English, Korean |
| 3 | OLIVER MASSMANN | Partner - Duane Morris Vietnam LLC | Alternative Dispute Resolution (ADR), Investment, International Trade, Banking & Finance, Insurance, Securities, Construction, Information Technology, Taxation services | Vietnamese, English, German |
| 4 | TO, WING CHRISTOPHER | Barrister-at-Law, Gilt Chambers | Alternative Dispute Resolution (ADR), Banking & Finance, Construction, Aviation, Information Technology, Intellectual Property | English, Chinese |
| 5 | NGUYEN THI THUY HANG | Deputy Director General, Public Procurement Agency, Ministry of Finance | Commerce, International Trade, Infrastructure, Construction, | Vietnamese, English, Japanese |
| 6 | To Van Hoa | Rector – Hanoi Law University | Alternative Dispute Resolution (ADR), Infrastructure, Construction, Information Technology, Intellectual Property | Vietnamese, English |
| 7 | NGUYEN TUAN HOA | Chairman of the expert panel, Vietnam Institute for Digital Economy Development | Information Technology | Vietnamese, English, Russian, French |
| 8 | TRAN MANH HUNG | Managing Partner and Director – BMVN International LLC | Franchise, Information Technology, Intellectual Property | Vietnamese, English |
| 9 | Tran Van Tung | Deputy Minister of Science and Technology | Information Technology | Vietnamese, English |
| 10 | LUU XUAN VINH | Director/ Managing Partner, Asia Legal Business Law Firm | Arbitration, Mergers and Acquisitions, International Trade, Construction, Information Technology | Vietnamese, English |

# Q&A

E: vinh.luu@asialegal.vn

M: 091 626 3656

W: asialegal.vn | dataprivacy.vn

**[VIAC x AUSCHAM WEBINAR SERIES 2026]**

## Topic 03 – AI, Digital Transformation and Cyber Resilience: What Businesses in Vietnam Should Prepare For?

---

## Q&A SESSION

### PART I: AI Adoption, Leadership and Organisational Readiness

***Question 1.1:*** *When companies assess AI risks, are they focusing on where the real operational risks actually sit, or are they becoming so fixated on legal compliance that they miss the bigger picture?*

**Mr. Colin Blackwell:** It is a natural aspect of human psychology to focus on problems that are easier to define and resolve. Policies, governance frameworks, and compliance requirements are relatively tangible and can be addressed through documentation and internal procedures. As a result, companies often devote considerable attention to these areas, particularly because responsibility can be distributed across established processes and functions.

However, the most significant risks may lie elsewhere. A company may, for example, face the risk of being overtaken by a competitor and ultimately become commercially unsustainable. Such risks are far more consequential, but they are also more difficult to confront because they involve uncertainty, competing interests, and difficult strategic decisions. Organisations therefore tend to focus more heavily on internal risks, which are easier to analyse, than on external risks that may pose a much greater threat to the business.

In reality, external risks can be substantially more serious. If a company fails because it has not adapted quickly enough or has lost its competitive position, its internal policies and compliance procedures will no longer be of practical relevance. Companies should therefore avoid analysing manageable risks in excessive detail while overlooking the broader threats that could fundamentally affect business continuity.

***Question 1.2:*** *What should business leaders do, personally and practically, to get themselves up to speed on AI quickly enough to lead, rather than simply react?*

**Mr. Colin Blackwell:** AI is, in many respects, remarkably straightforward to use. Interacting effectively with AI does not necessarily require advanced technical expertise; rather, it relies on many of the same skills that leaders already use in management, such as delegating tasks, reviewing outputs, defining objectives, and understanding the relevant context.

Many CEOs and senior executives initially assume that they are not well-suited to using AI because of their age or limited technical background. However, AI is not fundamentally a matter of technical proficiency. Experienced leaders are often already well equipped to use it because communicating with AI is, in many ways, similar to directing and managing employees. They must explain the objective, provide appropriate context, review the work produced, and determine whether the outcome meets the organisation's needs.

Nevertheless, the responsibility for leading AI adoption cannot simply be delegated. Business leaders must engage with the technology directly and develop a practical understanding of its capabilities and limitations. In my experience, CEOs and business owners often become highly enthusiastic once they realise that AI is more accessible than they had assumed. They begin identifying opportunities to automate processes because they have a direct interest in improving the organisation's performance and driving meaningful changes.

By contrast, employees may, consciously or unconsciously, be concerned about protecting their existing roles or preserving established manual processes. If leaders delegate responsibility for AI adoption entirely to others, they may encounter resistance, receive incomplete advice, or make decisions without a sufficient understanding of the technology.

A recent example illustrates this risk. A relatively simple AI automation, which could be completed in approximately five minutes and was demonstrated as part of a free service, was presented to a large software provider for implementation. Because the person requesting the service did not appear to understand the technology, the provider proposed a fee of **USD 1.2 million** and an implementation **period of 18 months**.

A business leader who approved such a proposal could expose the company to serious financial and governance consequences. A country manager, for example, might later be required to justify the decision during an internal audit. Claiming a lack of technical knowledge would not provide an adequate explanation and could raise further questions regarding the decision-making process and the relationship with the vendor.

Accordingly, CEOs and business owners do not need to become AI experts, but they must acquire sufficient practical knowledge to evaluate proposals, challenge unrealistic estimates, and protect the organisation from poor advice or opportunistic conduct. The most effective starting point is therefore simple: leaders should begin using AI themselves, become familiar with how it works, and remain personally involved in directing its adoption within the organisation.

***Question 1.3:*** *In the world of Agentic AI, do we still need humans?*

**Mr. Sam Russell-Vick:** There is a widespread concern that AI may eventually replace human workers and leave many roles obsolete. Recent reports concerning AI models behaving unexpectedly or attempting to circumvent safeguards have understandably added to these concerns.

However, I take a more optimistic view. Humans will continue to play an essential role and are unlikely to be fully replaced by AI. As Colin noted earlier in his presentation, regulatory frameworks already require human oversight in certain contexts, reflecting the importance of maintaining a human in the loop.

Beyond regulatory requirements, effective use of AI depends on human direction. AI does not inherently understand an organisation's motives, priorities, or ultimate objectives. To obtain meaningful results, users must define the relevant parameters, provide clear instructions, and guide the system towards the intended outcome.

The same principle applies when managing an organisation. A company cannot simply hire hundreds of employees and expect the business to grow automatically. Leadership must establish a clear direction, communicate the organisation's objectives, and provide the necessary guidance. AI similarly requires human direction and oversight to operate effectively.

Accordingly, individuals and organisations that are better able to direct, supervise, and use AI will gain a significant advantage over those that are not. For this reason, I remain optimistic that humans will continue to be indispensable, particularly in setting objectives, exercising judgment, and ensuring that AI is used responsibly and effectively.

***Question 1.4:*** *Among the three obligations outlined by Mr. Colin Blackwell – Classify, Disclose, and Control – as set out in Articles 9–15 and 34–35 of Law No. 134/2025/QH15, which do you consider the most challenging for businesses to implement in practice, and why?*

**Mr. Colin Blackwell:** Classify and disclose the AI can help companies with easily. As the AI has been used to build a process automation, it is simple housekeeping to ask the AI to document its own processes in a format consistent with AI laws. The challenging part is as usual human - controlling that the person designated to own that AI workflow and regularly conduct the human in the loop review steps - that they actually do it, records it and have the evidence of that in a readily accessible auditable format.

---

## PART II: AI Governance, Responsible Use and Liability

***Question 2.1:*** *In Vietnam, more than 97.5% of businesses are small and medium-sized enterprises. As a small business owner, I heard a lot about the risks of AI. If the leader wants staff to start using AI tools like ChatGPT to improve productivity starting tomorrow, what is the bare minimum step the leader should take to ensure we don't accidentally leak sensitive customer data, without needing a massive budget or a full-time legal team?*

**Mr. Luu Xuan Vinh:** This is a highly relevant and frequently raised question, particularly for small and medium-sized enterprises. In my view, businesses do not necessarily require a substantial budget or a full-time legal team to begin using AI tools more safely and responsibly.

The first and most important step is to move employees away from free public or personal accounts and onto an enterprise or team-based version of the relevant AI platform. These versions are generally designed to provide stronger data protection and subject to the applicable service terms, prevent business data from being used to train the underlying models.

The second step is to issue a clear internal instruction or memorandum governing the use of AI. Employees may be permitted to use AI tools for work-related purposes, but they should be expressly prohibited from entering personal data, confidential business information, or other sensitive material into prompts. This includes names, addresses, telephone numbers, client information, employee data, and internal documents.

Where the use of such information is necessary, employees should first remove, anonymise, or redact any details that could identify clients, business partners, employees, or other individuals. The purpose is to ensure that sensitive information is not disclosed to a public or external AI system.

By implementing these two basic measures – using an appropriate business account and establishing a clear rule against entering sensitive data – SMEs can begin using AI tools to improve productivity without immediately incurring significant legal, compliance, or cybersecurity costs. These measures may not replace a comprehensive governance framework in the longer term, but they provide a practical and accessible starting point for responsible AI adoption.

***Question 2.2:*** *If my company's AI makes a mistake, for instance, by giving a customer incorrect advice that causes financial loss, and the customer demands compensation, what should our immediate response strategy be? How do we balance apologising for the customer's loss without exposing the company to unnecessary legal liability?*

**Mr. Luu Xuan Vinh:** An incorrect response generated by AI can create significant legal, financial, and reputational consequences for a company. In such circumstances, the immediate response should be guided by empathy but should not amount to a premature admission of liability.

The company should avoid making statements such as, "***We are at fault because our AI system failed***", before the relevant facts have been properly investigated. Instead, it may respond by acknowledging the customer's concern and the impact of the incident, for example: "***We regret the inconvenience and loss caused by the information provided, and we have commenced an internal investigation to determine the cause of the incident***".

This approach allows the company to demonstrate that it is taking the matter seriously while preserving the opportunity to establish what actually occurred. The investigation should determine whether the incorrect advice resulted from an AI hallucination, inadequate system configuration, insufficient human oversight, inaccurate input, or user error. By investigating rather than immediately admitting a defect, the company can respond responsibly without unnecessarily prejudicing against its legal position.

At the same time, the matter should be promptly transferred to a qualified human representative. A person should review the advice generated by the AI, assess the customer's circumstances, and provide accurate guidance or an appropriate remedy. This human-in-the-loop response is essential not only for risk management, but also for restoring the customer's confidence.

In many cases, what the customer primarily seeks is a timely, accurate, and human-led resolution. The company should therefore combine a careful initial response with prompt investigation, effective human intervention, and clear communication throughout the process.

***Question 2.3:*** *In the Air Canada chatbot case, the AI-generated misinformation caused both financial and reputational damage. From a public relations and crisis-management perspective, how should a company respond immediately when a customer-facing AI system provides materially incorrect information? In addition, does Decree 356 prescribe any specific reporting obligation or timeline for such an incident?*

**Mr. Luu Xuan Vinh:** In the Air Canada chatbot case, the AI-generated misinformation caused both financial and reputational damage. From a public relations and crisis-management perspective, when a company's AI generates erroneous advice resulting in a customer's financial loss, the optimal strategy requires balancing customer empathy with legal risk management. The company's immediate response must separate customer service from legal admissions of fault. The company should swiftly validate the customer's frustration by apologizing for their negative experience but strictly avoid apologizing for the actual mistake or admitting that the AI was incorrect, and concurrently, transfer the matter to technical experts to investigate the root cause and provide an appropriate commercial remedy.

If the company's investigation confirms the AI was at fault and the customer's reliance was reasonable, the most prudent approach is to resolve the matter commercially rather than legally. This strategy effectively repairs the customer relationship while keeping the dispute out of the courtroom and the headlines.

Decree No. 356/2025/ND-CP, which took effect on January 1, 2026, serves as the guiding framework for Vietnam's Law on Personal Data Protection (PDPL). It specifically addresses personal data protection regimes in modern technology fields, including Artificial Intelligence and Big Data. Whether an AI misinformation incident triggers a reporting obligation under Decree 356 depends entirely on the nature of the AI's error. Specifically, if the company suffers an actual or suspected data breach, they must notify the Specialized Authority for Personal Data Protection (A05) within 72 hours of becoming aware of the incident. If the AI system hallucinates business information, false advice, or incorrect pricing (like the Air Canada case), but does not compromise personal data, it is a consumer protection issue rather than a data privacy issue. As no personal data was leaked, altered, or unlawfully processed, the 72-hour reporting obligation under Decree 356 does not apply.

## PART III: Emerging Cybersecurity Risks in the AI Era

***Question 3.1:*** *Could you explain what Large Language Model (LLM) jacking looks like in practice? Does it primarily involve attackers stealing API credentials to generate unauthorised usage costs, or does it extend to other forms of misuse? How frequently is this now appearing as a cyber claim?*

**Mr. Sam Russell-Vick**: This misuse can take several forms, all of which result in excessive or unauthorized consumption of compute, including:

- Running unauthorized AI workloads using stolen access
- Training or fine-tuning large models for commercial or malicious use
- Extracting proprietary training data or model weights through compute-heavy probing
- Manipulating model outputs to serve malicious content – particularly when such misuse leads to sustained or abnormal resource usage

Regarding LLMJacking claims frequency. Because this is a relatively new cyber-attack vector, our data capture is relatively short. However, I can say for QBE, we have seen an increase in claims frequency from LLMJacking related incidents across Asia this year.

Please refer to our LLMjacking information sheet (attached) for more details.

***Question 3.2:*** *Why do you think there has been a rise in ransomware activity in the legal sector?*

**Mr. Sam Russell-Vick:** This is an issue that QBE has considered carefully. In our assessment, one of the principal reasons for the increase in ransomware activity targeting the legal sector is the highly sensitive and valuable nature of the information held by law firms.

Legal practices routinely retain confidential client communications, commercially sensitive documents, privileged material, transaction records, and information relating to ongoing disputes. The unauthorised disclosure of such information can therefore cause significant reputational damage, both to the law firm and to its clients.

From the perspective of cybercriminals, this creates a stronger incentive for law firms to pay a ransom than may exist in other sectors, particularly where the stolen information would be highly compromising if disclosed publicly. In effect, the issue reflects a supply-and-demand dynamic: because law firms are under a particularly strong obligation to preserve confidentiality, attackers may consider them more likely to make payments in order to prevent the release of sensitive data.

We believe that this heightened pressure to protect confidential information is one of the systemic factors contributing to the global increase in ransomware incidents and ransom payments involving legal firms.

***Question 3.3:*** *I'm also the founder of a law firm, and I usually see ransomware attackers targeting large - scale companies rather than law firms. Law firms in Vietnam, for example, are generally quite small. Is there any other reason behind that?*

**Mr. Sam Russell-Vick:** That is an important observation. Traditionally, ransomware groups tended to focus on larger organisations. However, the increasing use of AI and automation has significantly changed the economics and scale of cyberattacks.

Attackers can now automate large parts of the process and target a much broader range of organisations with relatively little additional effort. In practice, they are often less concerned with the size or identity of the victim than with whether the organisation can be successfully extorted.

Whether the target is a major corporation, an insurer, a law firm, or another business, the determining factor is often the likelihood that the attack will produce a financial return.

We are therefore seeing a growing number of incidents involving SMEs. Smaller organisations generally have fewer resources to invest in sophisticated cybersecurity systems, specialist personnel, and advanced monitoring technologies. As a result, they may present easier targets for cybercriminals and become the “lowest-hanging fruit” within the threat landscape.

From the attacker’s perspective, ransomware operates as a business model. Cybercriminals seek to maximise their return while minimising the time, cost, and technical effort required. If an SME can be compromised relatively easily and remains capable of making a substantial payment, it may be considered an attractive target. In some cases, attackers may even prefer SMEs because their security controls are less developed than those of larger organisations.

There is also an important financial dimension for business owners. SMEs must maintain sufficient working capital to pay employees and meet their operational obligations. A ransom demand amounting to hundreds of thousands of US dollars can therefore create an immediate and potentially severe liquidity crisis.

For this reason, ransomware is not merely a technical or cybersecurity issue for SMEs. It is a direct threat to business continuity and can become a highly personal concern for founders, CEOs, and business owners who are responsible for ensuring that the organisation continues to operate.

---

**PART IV: Dispute Readiness and the Strategic Use of ADR**

***Question 4.1:*** *When disputes involving AI, cybersecurity, digital platforms, or technology contracts arise, why may arbitration be the best choice?*

**Mr. Luu Xuan Vinh:** As I mentioned in my presentation, when resolving complex technology disputes, commercial arbitration offers four distinct advantages over traditional litigation:

- *First*, arbitration allows parties to select tech-savvy adjudicators. Unlike standard court judges, who frequently lack the specialized technical background required to interpret complex source code, understand the intricate "black box" of AI algorithms, or decipher how smart contracts actually function, arbitrators can be hand-picked for their specific engineering and technological acumen. This ensures the decision-maker truly understands your product and avoids technically flawed rulings.
- *Second*, arbitration guarantees absolute confidentiality, which is the lifeblood of the tech industry. While traditional court proceedings are inherently public – risking the catastrophic exposure of sensitive intellectual property, proprietary business strategies, and private client lists to the press or competitors – arbitration's default privacy protects this vital trade data from start to finish.
- *Third*, arbitration provides crucial procedural flexibility and advanced e-discovery, where arbitral tribunals can establish tailored procedural orders, allowing parties to agree on customized data extraction methodologies, authorize the use of AI for Technology-Assisted Review, and efficiently verify forensic digital evidence like server log files.
- *Finally*, arbitration ensures global enforceability. Enforcing a national court judgment across borders is a notoriously difficult, multi-layered bureaucratic process. However, thanks to the 1958 New York Convention, arbitral awards are legally recognized and readily enforceable in over 170 countries. In today’s interconnected digital economy where a single cross-border technology contract frequently involves parties, offshore developers, and

international clients, this borderless enforceability acts as your "golden key," offering the most reliable mechanism to secure commercial rights and protect investments when a global partner defaults.

***Question 4.2**: (Q 2.3 cont.) Do you expect Vietnamese courts and arbitral tribunals to draw guidance from foreign cases such as the Air Canada chatbot case when assessing liability for AI-generated misinformation, or is Vietnam likely to develop a distinct approach?*

**Mr. Luu Xuan Vinh**: From my point of view, Vietnamese courts and arbitral tribunals will likely look to landmark foreign rulings, such as the Air Canada chatbot case, as strong persuasive guides. These international precedents establish a vital commercial baseline: companies cannot dodge legal responsibility for the mistakes made by AI systems they deploy. If an enterprise uses an AI tool to benefit its business, it must take ownership of any erroneous information that system generates.

However, one thing to note is that as Vietnam is a civil law jurisdiction, courts and tribunals will not rule based on foreign case law alone. Instead, they will anchor those global principles firmly within Vietnam's codified laws. Vietnamese courts and arbitral tribunals will evaluate AI liability using three main legal pillars:

- The Civil Code 2015: This will be used to assess faults and handle breaches of contractual obligations caused by AI errors.
- Consumer Protection Regulations: These rules will be applied to shield users from misleading information or unfair practices resulting from corporate AI tools.
- The Law on Artificial Intelligence (Law No. 134/2025/QH15): This specific legislation will be used to enforce corporate duties surrounding AI transparency and control.

In short, while the underlying logic in these disputes mirrors global trends, the final judgments will be deeply rooted in Vietnam's specific statutory framework.

***Question 4.3**: From an arbitrator's perspective, how difficult is it in practice to establish that a cyberattack was deliberately staged rather than caused by a genuine external breach? What forms of forensic evidence and technical expertise are generally most persuasive in such cases?*

**Mr. Luu Xuan Vinh**: It is very difficult for an arbitrator to prove that a company faked a cyberattack to get out of trouble or hide evidence. Faking an attack is basically fraud, which requires very strong proof. The biggest problem is that the accused company owns the computers and controls the initial investigation, giving them a huge advantage. It is also tough to tell the difference between a rogue employee and a real hacker who bought a stolen password, especially since any major computer breach is naturally chaotic and confusing.

To figure out the truth, the arbitrator will look for hard computer evidence showing the "hackers" didn't act like real cybercriminals. Fake attacks often look sloppy. For example, the ransomware might not actually work, or the only files destroyed just happen to be the exact documents needed for the lawsuit. It is also very suspicious if the attack started from a computer inside the company's own building in the middle of the night, or if someone turned off the antivirus software right before the hack happened.

Since the arbitrators are not computer experts, they must rely on independent cybersecurity investigators and independent digital forensics and incident response firms to accurately interpret this data. They can tell a clear story, showing how the "attackers" skipped normal steps that real hackers always have to take which strongly points to an inside job. Ultimately, these experts have to prove that the attack just does not make sense for a real hacker looking to make money. This may help the arbitrators see that the highly convenient timing of the "hack" was no accident.

## BIBLIOGRAPHY

### A. Treaties and Legislation


1. Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 330 U.N.T.S. 3 (New York Convention).
2. Law on Artificial Intelligence 2025 (Law No. 134/2025/QH15). (2025).
3. Law on Cybersecurity 2025 (Law No. 116/2025/QH15). (2025).
4. Law on Data 2024 (Law No. 60/2024/QH15). (2024).
5. Law on Digital Transformation 2025 (Law No. 148/2025/QH15). (2025).
6. Law on Personal Data Protection 2025 (Law No. 91/2025/QH15). (2025).
7. Civil Code 2015 (Law No. 91/2015/QH13). (2015).
8. Decree No. 13/2023/ND-CP on Personal Data Protection. (2023).
9. Decree No. 356/2025/ND-CP Detailing the Law on Personal Data Protection. (2025).
10. Foreign legislation and regulatory instruments
11. Personal Data Protection Act 2012 (Singapore). (2012).


### B. Publications


1. Baker McKenzie. (2025). *Annual disputes survey: Technology-related issues top 2025 disputes risk*. Baker McKenzie. https://www.bakermckenzie.com/en/newsroom/2025/01/baker-mckenzie-annual-disputes-survey
2. Baker McKenzie. (2025). *Global disputes forecast 2025*. Baker McKenzie. https://www.bakermckenzie.com/-/media/files/insight/publications/2025/01/global-disputes-forecast-2025.pdf
3. Hạ, C. (2026). *Over 50% of agencies and businesses hit by cyberattacks in 2025*. VnEconomy. https://en.vneconomy.vn/over-50-of-agencies-and-businesses-hit-by-cyberattacks-in-2025.htm
4. IBM Security. (2025). *Cost of a data breach report 2025*. IBM. https://www.ibm.com/reports/data-breach
5. Sajadieh, S., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Santarlasci, L., Pava, J., Maslej, N., Altman, R., Brynjolfsson, E., Brodley, C., Clark, J., Dignum, V., Kumar, V., Landay, J., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Tabassi, E., Wald, R., Walsh, T., & Weld, D. (2026). *The AI Index 2026 annual report*. AI Index Steering Committee, Institute for Human-Centered Artificial Intelligence, Stanford University. https://doi.org/10.48550/arXiv.2606.15708
6. The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. The Economist. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
7. QBE Insurance Group. (2025). *Cyber threats: Legal and professional services sector*. QBE. https://www.qbe.com/media/qbe/shared/files/832467-lps-cyber-threat-whitepaper-final.pdf

8. QBE Insurance Group. (2025). *Reimagining commercial espionage and fraud in the era of agentic AI*. QBE. https://www.qbe.com/media/qbe/north-america/usa/pdf-files/research-and-insights/agentic-ai-report.pdf

**C. Cases**

**United States**

1. *Thaler v. Perlmutter*, No. 23-5233 (U.S. Court of Appeals for the District of Columbia Circuit, 2025).
2. *U.S. Equal Employment Opportunity Commission v. iTutorGroup*, No. 1:22-cv-02565 (E.D.N.Y. 2023).
3. *MD Anderson Cancer Center v. IBM Watson Health*, No. 4:18-cv-00634 (S.D. Tex. 2017).
4. *Heritage Valley Health System v. Nuance Communications, Inc.*, No. 2:20-cv-00631 (W.D. Pa. 2020).

**China**

5. *Li Yunkai v. Tencent Technology (Beijing Internet Court Judgment, 17 November 2023).*

**France**

6. *Paris Court of Appeal, Case No. 18/03616* (Judgment of 7 February 2020, France).

**Canada**

7. *Moffatt v. Air Canada*, 2024 BCCRT 149 (Can.).

---

**Disclaimer:**

*This material was prepared in connection with the webinar "**AI, Digital Transformation and Cyber Resilience: What Businesses in Vietnam Should Prepare For?**" for general informational and reference purposes only, including for lawyers, businesses, practitioners, and other interested stakeholders. The views and opinions expressed in this document are those of the respective speakers and experts in the context of the webinar and do not necessarily reflect the official position of the Vietnam International Arbitration Centre (VIAC) or the Australian Chamber of Commerce in Vietnam (AusCham Vietnam).*

*This material does not constitute legal, professional, or other advice and should not be relied upon as a substitute for advice tailored to specific circumstances. Any reference and citation to this research made by a third party shall not be valid or recognized by VIAC and/or AusCham Vietnam.*

Organized by

AUSCHAM VIETNAM

In Collaboration with

VIAC VIETNAM INTERNATIONAL ARBITRATION CENTRE

Powered by

enablecode ASIA LEGAL BUSINESS LAW FIRM QBE

WEBINAR

# AI, DIGITAL TRANSFORMATION AND CYBER RESILIENCE: WHAT BUSINESSES IN VIETNAM SHOULD PREPARE FOR?


AUSCHAM VIETNAM

Hanoi Office

13F, Hanoi Tower, 49 Hai Ba Trung, Cua Nam Ward, Ha Noi, Vietnam

+84 (0) 97 300 04 71

https://auschamvn.org

VIAC VIETNAM INTERNATIONAL ARBITRATION CENTRE

Hanoi Office

6th Floor, VCCI Tower, No.9 Dao Duy Anh St., Kim Lien Ward, Hanoi, Vietnam

+84 243 574 4001

https://viac.vn