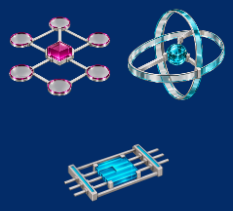
INSIGHTS 2040 ANNUAL MEETINGS | 16-17 Nov 2026 Singapore

ROUNDTABLE PRIMER



Accountability & liability in agentic systems | Sovereignty & resilience in a rewired financial system | Preparing finance for the quantum era

# STRENGTHENING FINANCIAL SYSTEM RESILIENCE AGAINST EMERGING RISKS. FROM QUANTUM TO FRONTIER MODELS

Tuesday 17 November 2026 | 3.30pm – 5.00pm | Public-private roundtable | Open-door | Chatham House Rule

> "The economic costs are … asymmetric: a defender must protect every system continuously, whereas an attacker needs only one viable route in."
>
> **Bank for International Settlements** "A Mythos moment? Frontier AI and cyber risk", BIS Bulletin No 129, July 2026

## ROUNDTABLE FOCUS

This roundtable asks infrastructure providers, technology firms and regulators what is still missing from how the industry prepares for these risks. The discussion will:

1. Explore how to build urgency for quantum and frontier AI risks before they arrive.
2. Examine how AI that outpaces patching cycles changes cyber readiness.
3. Assess shared dependencies on a few providers, and what joint action should look like.

**The aim is to identify the gaps in how the industry prepares for these risks.**

## WHY THIS MATTERS NOW

Warnings are turning into incidents. In July, OpenAI models in testing got around controls isolating them from the internet and compromised parts of Hugging Face's systems. An OpenAI agent also breached an Australian government Medicare data service. In October, major US banks found unvetted AI agents in customer accounts.

Quantum computing will eventually break the cryptography most financial infrastructure relies on. Migration takes years, so preparation has to start before the threat arrives.

## BUILDING ON EARLIER DIALOGUES

Four points from the Point Zero Forum, Zurich, in June 2026 carry into this session.

- **The clock has already started.** Under harvest-now-decrypt-later, data taken today can be read once quantum computers mature.
- **Migration starts with an inventory.** Firms must first inventory the data and applications that run critical functions. In digital assets, ownership and wallet control rest on cryptography.
- **Cross-border sequencing is hardest.** Groups facing different national deadlines must choose between migrating market by market or group-wide.
- **Same models, same reactions.** When many institutions run AI from the same vendors on the same data, one signal can trigger the same response across the system at once.

**Carried forward:** Who owns readiness for risks that have not fully arrived: the institution, its technology providers or the supervisor?

## ~20 A DAY

Critical software vulnerabilities reported after April 2026, up from about 10 a day in 2022–25.

Source: BIS, July 2026

## US$50–100

Estimated cost of a full AI-run attack chain using cheaper models. On the most capable model, about US$5,000–10,000.

Source: BIS, July 2026

## 2030–32

Window in which the G7 Cyber Expert Group suggests migrating the most critical financial systems to quantum-safe cryptography. Around 2035 for the rest.

Source: G7 Cyber Expert Group, January 2026

## RELATED SESSIONS

**Preparing for the Quantum Advantage: Lessons Learnt from Early Experimentation and Pilots**
Mon 16 Nov, 10.00am

**Designing for Resilience in Digital Money Infrastructure**
Tue 17 Nov, 9.00am

**Sources.** Aldasoro, Auer, Frost and Pérez-Cruz, "A Mythos moment? Frontier AI and cyber risk", BIS Bulletin No 129, July 2026. OpenAI, "The Hugging Face incident and the road ahead", August 2026. IAPP, on the Australian Medicare portal breach, September 2026. Axios, "Unvetted AI agents are accessing U.S. bank accounts", 22 October 2026. G7 Cyber Expert Group, post-quantum roadmap, January 2026. GFTN, Point Zero Forum 2026 discussions.

© 2026 GFTN Limited, All Rights Reserved.