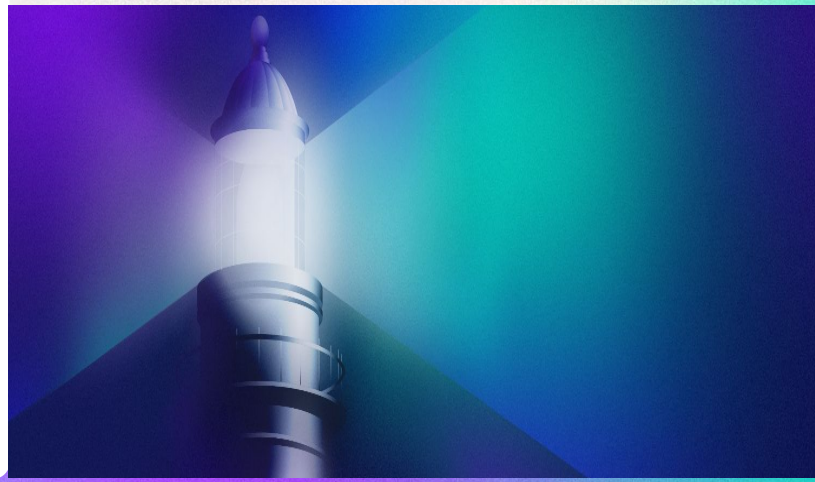
ISTARI Lighthouse

Governing Amid Geopolitical Disruption and Technological Change

Making Your Board Cyber Resilient

Professor Lucas Kello, ISTARI & Oxford University
Thai Institute of Directors | 9 September 2026



Today's three sessions

01 **The Changing Cyber Risk Landscape** — 50 min

Geopolitical disruption and rapid technological change

02 **Cybersecurity Resilience Framework** — 40 min

Building your foundation

03 **Preparing the Board** — 40 min

Case studies and lessons

01

The Changing Cyber Risk Landscape

Geopolitical disruption & technological change

A moment of inflection

GEOPOLITICAL DISRUPTION

- Multipolar rivalry
- State cyber campaigns
- Sanctions and supply-chain pressure

TECHNOLOGICAL ACCELERATION

- AI agents and automation
- Cloud and software concentration
- Quantum migration

Cyber risk is no longer mainly a technical issue. It is a strategic business risk.

Why this matters in Thailand now

01

Quantum-Ready 2030

National migration planning has begun.

02

Cloud security standard

New national standard takes effect on 10 September 2026.

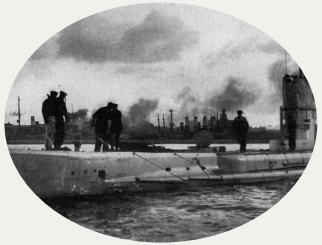
03

Direction of travel

From reactive defence to proactive resilience.

Technology changes faster than doctrine

Behind many strategic failures is a bad theory of new technology.



1914

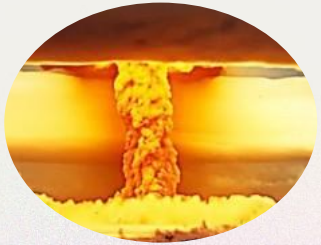
Submarine warfare

1937

Strategic air power

1940

Mechanised warfare



1945

Nuclear conflict

2007+

Cyber and AI

Institutions usually adapt after an initial shock.
By then, it's too late.

From nuisance to geopolitical convergence

Cyber threats have moved from isolated digital events to a fusion of geopolitical rivalry and technological disruption.

STAGE 0

Nuisance & crime

Basic malware; low-cost disruption

STAGE 1

Demonstration

First crises show political impact

STAGE 2

Industrial sabotage

Targeted damage to systems and operations

STAGE 3

Political subversion

Influence and narrative manipulation

STAGE 4

Convergence

Multipolar rivalry + AI + fragile interdependence

We are in the middle of the next phase shift.

The fifth transition

Power transition amid permanent technological change

1 Return of multipolar rivalry

- Competition moves beyond military domains.
- Digital and infrastructure pressure become tools of statecraft.

2 Permanent technological acceleration

- AI, cloud and digital dependence amplify fragility.
- The risk surface changes faster than static controls.

3 More conflict below the war line (unpeace)

4 Private infrastructure becomes strategic terrain

5 Governance and law keep lagging

A world of unpeace

Persistent conflict below the threshold of war—more harmful than normal competition, but short of open war.

01 Major powers avoid direct war

02 Pressure shifts into cyber, data, supply chains and influence

03 Companies become part of the contest

Source: Kello, *The Virftual Weapon and International Order (2017)*

The rise of corporate geopolitics

Private companies often believe they are outside geopolitics.

- Strategic assets attract state attention.
- Neutrality does not protect infrastructure, data or suppliers.
- Cloud, identity, software and logistics are now strategic terrain.

If your business is strategically relevant, geopolitics will come to you.

What strategic intrusion looks like

1 Stealth

No visible disruption. The actor avoids attention.

2 Persistence

Access is maintained for months or years.

3 Pre-positioning

Leverage is saved for a future crisis.

Recent patterns

Email-system compromise • Telecom surveillance • Satellite disruption

The objective is often access and leverage—not ransom.

AI changes the offence–defence balance

1

Hacking with AI

Faster phishing, impersonation, malware changes and vulnerability search.

2

Hacking the AI

Prompt injection, data poisoning, tool hijacking and model theft.

3

Hacking for AI

Steal data, logs, models and compute to improve offensive systems.

AI-augmented threats are here. Agentic systems raise the tempo again.

The next wave: delegated action

LLM as tool

User asks.
Model responds.
Human acts.

Copilot

Model proposes.
Human approves.
System executes.

Agentic AI

Goal persists. Model plans.
Tools act. Human intervenes
by exception.

Goal → **Plan** → **Tools** → **Memory** → **Action**

Control = permissions, visibility, containment, rollback and human authority.

Quantum risk starts before “Q-Day”

Harvest now, decrypt later

Encrypted data stolen today may become readable later.

Long-lived data creates a present-day board risk.

What boards should do now

- Map long-lived data
- Build a cryptographic inventory
- Set a migration owner and timetable

Thailand’s Quantum-Ready 2030 makes this a current governance issue.

Sources: NIST; Thailand NCSA Quantum-Ready 2030

Govern in dynamic probabilities

Static maturity scores show where you were. They do not show what may hit next.

1 Vision

Are we looking ahead—or only reporting the past?

2 Exposure

Which critical services and assets matter most?

3 Foresight

What event would force us to change posture?

4 Ecosystem

Which partners must respond with us?

SESSION 1 TAKEAWAY

What directors should now assume

01 Intrusion is a starting assumption of security strategy

02 Disruption can spread across the group and supply chain

03 AI will compress decision time

04 Regulation will keep moving, including into the boardroom

05 Resilience depends on adaptation before a crisis

02

Cybersecurity Resilience Framework

Building your foundation

Mindshift: From security to resilience

CYBERSECURITY

- Keep the attacker out
- Protect systems
- IT-led
- Point-in-time assurance

CYBER RESILIENCE

- Assume some intrusion
- Keep critical services running
- Enterprise-led
- Continuous learning

Prevention remains essential. It is no longer sufficient.

Cyber resilience means the ability to...

Anticipate

See emerging threats

Withstand

Limit operational impact

Respond

Decide under uncertainty

Adapt

Recover and emerge stronger

The goal is to master the anticipation game.

Resilience is built by routine

Five leadership routines turn resilience from an idea into a management system.

1

Strategy

Critical services
Risk appetite

2

Culture

Shared responsibility
Speak-up

3

Organisational design

Roles
Decision rights

4

Risk & governance

Playbooks
Metrics & exercises

5

Ecosystem

Suppliers
Regulators & support

Resilience is a repeatable management system—not a one-off project.

HELM: a boardroom framework for proactive resilience

H

Horizon Scanning

What is changing?

E

Enterprise Governance

Who decides—and how?

L

Leadership Culture

How do leaders behave?

M

Monitoring

What does the board track?

HELM connects foresight, decision rights, culture and oversight.

Eight steps for the board

1. Understand the board's role
2. Assess maturity and risk appetite
3. Embed cyber in enterprise risk
4. Build the fundamentals
5. Secure digital transformation
6. Close capability gaps
7. Maintain oversight
8. Recover and learn

Use this as a cycle, not a one-time sequence.

Checklists are just the floor. The ceiling is higher.

CHECKLIST

Defines minimum questions and evidence

→

PLAYBOOK

Clarifies roles, thresholds and decisions

→

EXERCISE

Tests judgement, pressure and coordination

A checklist can show that a plan exists. Only practice shows whether it works.

What Regulators Are Worried About

01	**Geopolitical instability and state-linked campaigns**	Prepositioning for future disruption, not just stealing data
02	**Complex supply chains and interdependent infrastructure**	Regulators do not believe risk sits only within the enterprise ‘perimeter’
03	**Transformation of business models and services**	AI, Cloud – services increasingly run on infrastructure the company does not own, operate or see
04	**Attackers moving faster than defenders can respond — the new pressure**	AI cuts the time to find a vulnerability and build an exploit from months to hours
05	**Cryptography with an approaching quantum expiry date**	Data being harvested today can be decrypted later

How Obligations Are Widening and Quickening: Accountability, Perimeter and Pace Increase

01

From paperwork & disclosure to preparedness & demonstrable governance, especially by boards.

- Raising expectations on boards, eg for critical sectors in Europe, Singapore and Australia. Directors set tone and accountability for cyber risk.
- Eg, Singapore requires critical infrastructure owners to run exercises, set board-approved risk tolerances, and train directors annually

02

The ‘perimeter’ keeps descending into the infrastructure beneath you

- UK is pulling managed service providers and data centres into scope. Singapore is looking to regulate major cloud providers and data centres.
- Europe now regulates the security of connected products sold into the EU – reporting from Sep 2026, full requirements from Dec 2027

03

Reporting is broadening and the clocks are shortening

- Reporting clocks now run in hours, not days — 24 to 72 hours across Europe and the UK, down to six hours in Malaysia and two in Singapore
- Australia requires ransomware payments to be reported within 72 hours (above A$3m turnover)

Deepening and Crossing Borders: From Advice to Supervision and Beyond

01 AI and Quantum risks were handled by advisories. It is moving to supervision and obligation.

- Europe's high-risk AI rules pushed back to December 2027, and to August 2028 for AI built into regulated products
- Singapore intends to supervise rather than legislate on AI risk for financial institutions. It expects its financial sector to be quantum-resilient before the end of this decade
- The US has set hard quantum deadlines of 2030 and 2031 for its own federal government systems, and requires a machine-readable register of cryptographic dependencies
- Switzerland expects its banks to have a board-approved quantum migration roadmap by mid-2027

02 Technology export rules & foreign obligations go deeper

- US export rules used to turn on where hardware shipped; new guidance is looking at who ultimately owns the buyer
- Foreign obligations can arrive through supplier contracts and counterparty requirements - before a domestic regulator does so

Regulatory demands will generally continue to grow globally. The timeline may change, but don't expect the general direction to.

03

Preparing the Board

Case studies and lessons

Worst practices: why crisis control fails

1. No clear owner
2. Slow or unclear escalation
3. Conflicting communication
4. No workable fallback
5. Board absent—or becomes a bottleneck

A crisis is not the time to debate who is in charge!

Best-practice case: Norsk Hydro (2019)

Global ransomware attack across IT and operations

What worked

- Clear emergency structure
- Manual workarounds protected operations
- Open, frequent communication
- Systems rebuilt from backups; lessons applied

Best practice is not avoiding disruption. It is controlling the consequences.

Resilience warning: Jaguar Land Rover (2025)

JLR

5+ weeks before phased manufacturing restart

£196m cyber-related costs reported in Q2

£1.5bn government-backed loan guarantee for supply-chain support

Board lessons

- Digital outages can halt physical production
- Supplier resilience becomes enterprise resilience
- Recovery priorities must be agreed before the crisis
- Use realistic timelines—not optimistic promises

Ask: could your business operate for five weeks without core systems?

Best practices when it matters most

BEFORE THE CRISIS

- Clear activation triggers
- Roles and decision rights
- Tested fallback procedures

DURING THE CRISIS

- Daily decision rhythm
- Fact-based communication
- Regulator and stakeholder coordination

AFTER THE CRISIS

- Independent review
- Close actions to completion
- Update playbooks and exercises

Readiness turns crisis from improvisation into controlled action.

What Thailand's Recent Breaches Reveal

3,180

cyber-attacks per week on average — around 70% above the global average

THB 21.5m

in PDPA fines across five cases in 2025 — up from near-zero a year earlier

2.2m+

Thai citizen records exposed in a set of cyber incidents

WHAT THE CASES REVEAL

Identity & access: Weak passwords and incomplete MFA turn stolen credentials into primary entry points.
Third-party exposure: Processors and vendors extend the attack surface while obscuring accountability.
Basic hygiene gaps: No DPO and lack of reporting draw the largest regulatory fines.
Readiness: Weak detection and response discipline magnify operational and regulatory impact.
Ransomware speed: Attackers move from breach to encryption in under 14 hours.
Stolen data: Information is active and resold as a service via chat bots.
Trust is the largest cost: Customer and citizen confidence outlasts any single fine.

#1

Business Disruption Risk (2026)

Up from #5 in 2025

3x

More Ransomware Attacks

Affecting Thai businesses in the past two years

Sources: Check Point 2024–25; PDPC / DLA Piper 2025; Nation Thailand & Bangkok Post 2025; Allianz Risk Barometer, ThaiCERT 2025.

New Rules Reshaping the Board's Cyber Agenda

CYBER

Cybersecurity Act CII duties (2024): 24-hour incident reporting, annual audits and board-approved frameworks. PDPA: 72-hour breach notice, fines to THB 5m.

IMPACT

Enforced accountability across seven critical sectors.

AI

Draft AI Law (ETDA, 2025; enactment ~2028), risk-based like the EU AI Act. Sector rules already live — Bank of Thailand AI risk management, AI-ad and court disclosure.

IMPACT

Formal AI governance expected now, ahead of the law.

QUANTUM

National quantum roadmap and post-quantum warnings from NCSA, ETDA and NSTDA. "Harvest now, decrypt later" flagged as a present-day risk to encrypted data.

IMPACT

Begin crypto-agility and post-quantum migration planning.

CLOUD

"Cloud First" policy live 2025 via the government cloud (GDCC). Draft cloud cybersecurity standards for CII and providers, with data-classification duties.

IMPACT

Data sovereignty, classification and vendor assurance.

WHAT THE BOARD NEEDS TO PREPARE FOR

- Govern cyber, data and AI as one board-level agenda across overlapping laws — not separate IT projects.
- Stand up AI governance and third-party risk oversight now, ahead of the AI law.
- Rehearse incident response routines when stakes are low; embed cyber resilience by routine

THREE DECISIONS FOR THE NEXT 12 MONTHS

- Name accountable executives for cyber, privacy, AI and cloud.
- Test applicable 24-/72-hour reporting pathways and third-party escalation. Conduct senior level tabletop exercise.
- Fund cyber resilience maturity assessment, cryptography inventory and cloud data-classification work.

Sources: Tilleke & Gibbins; Baker McKenzie; DLA Piper; Lexology; NCSA / ETDA; Bangkok Post 2024–2026.

Five decisions to pre-agree

1. Who leads the enterprise response?
2. What triggers board activation?
3. Which services are restored first?
4. Who approves shutdowns, payments and disclosure?
5. How are regulators, customers, employees and suppliers informed?

Board role: oversight and strategic decisions—not running the technical response.

Build a Board-Level Master Playbook