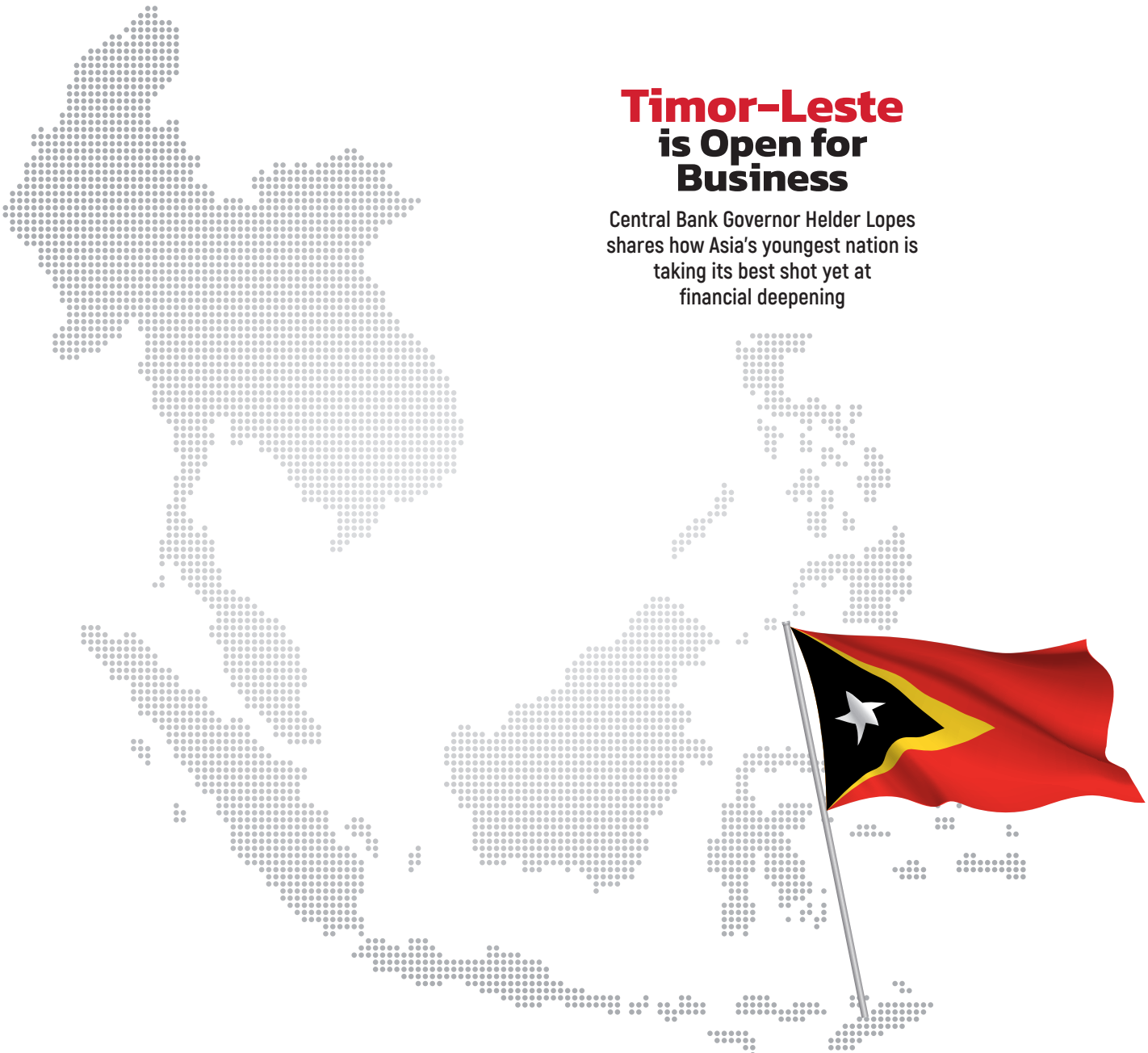
Angus Salim bin Salleh Amran, FCB, Group Chief Sustainability Officer at RHB Bank Bhd and Vice President of the Financial Markets Association of Malaysia
High Ethical Financial Leadership

BANKING INSIGHT

IDEAS FOR LEADERS | JUNE 2025

PP 17327/05/2013(032407)



Timor-Leste is Open for Business

Central Bank Governor Helder Lopes shares how Asia's youngest nation is taking its best shot yet at financial deepening

A PUBLICATION OF

AICB
ASIAN INSTITUTE OF CHARTERED BANKERS

ISSN 2231-6264

Are We Still Kicking Away the Ladder?

STRENGTHENING OPERATIONAL RESILIENCE AGAINST THE EVOLVING THREAT LANDSCAPE

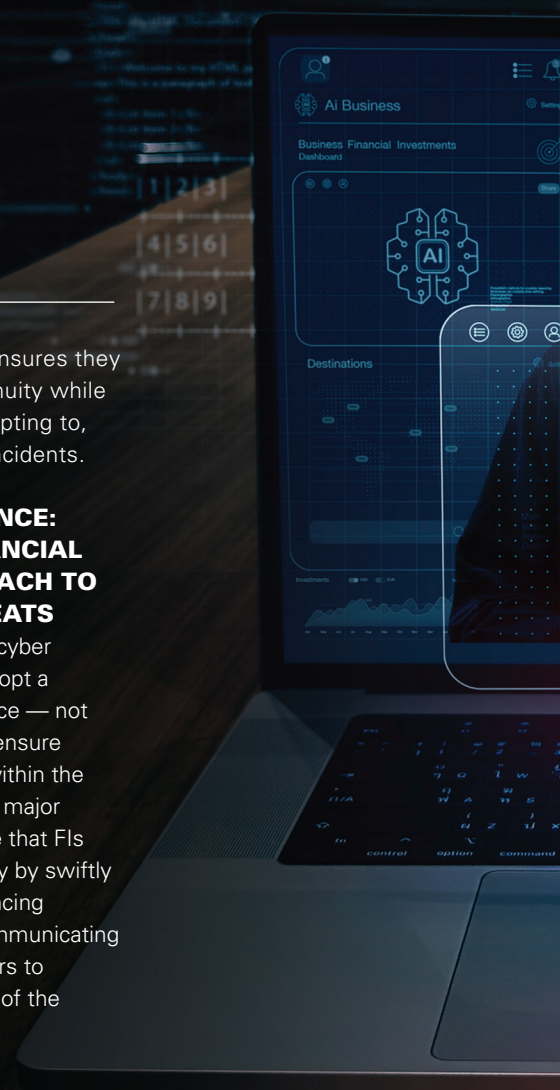
THE ETHICS OF LENDING

STRENGTHENING OPERATIONAL RESILIENCE

Against the Evolving Threat Landscape

By Christophe Barel

THE ANSWER IS A BROAD, MULTI-LAYERED, AND PROACTIVE RISK MANAGEMENT STRATEGY.



Cyberthreats are escalating in both scale and sophistication, and AI-driven attacks, ransomware, and phishing schemes are increasingly successful. There was a 15% year-on-year increase in cyberattacks in Asia Pacific (APAC) in 2024, with organisations in the region experiencing an average of 1,963 attacks per week. The financial sector is the fourth-most commonly targeted by ransomware in APAC.

Threat actors have sophisticated tools, allowing even the less skilled to mount effective attacks, and no financial institution (FI) can thwart 100% of them. For this reason, FIs must focus on building a comprehensive resilience strategy that combines strong digital defences that are reinforced by multiple layers of safety nets. This approach ensures they can maintain business continuity while effectively preparing for, adapting to, and recovering from cyber incidents.

OPERATIONAL RESILIENCE: THE BEDROCK OF FINANCIAL INSTITUTIONS' APPROACH TO CYBER RISK AND THREATS

Given the rapidly changing cyber threat landscape, FIs must adopt a proactive approach to resilience — not just to survive attacks but to ensure long-term stability and trust within the financial ecosystem. During a major cyber incident, it is imperative that FIs maintain operational continuity by swiftly isolating vulnerabilities, enhancing monitoring protocols, and communicating transparently with stakeholders to maintain trust — the bedrock of the financial services sector.

Such resilience can be achieved by a commitment to strong infrastructure, systems, frameworks, and organisational culture, with constant review and improvement. Resilience isn't an outcome — it's an activity that has to be conducted every day.

BEST PRACTICES TO ENHANCE OPERATIONAL RESILIENCE

Enhancing operational resilience in FIs begins with a strong foundation in cyber hygiene. Implementing measures such as multi-factor authentication, proactive threat monitoring, timely vulnerability patching, and robust network security controls are essential steps. These practices not only protect critical systems but also ensure compliance with evolving regulatory frameworks across the Asia Pacific region.

Beyond technical safeguards, fostering a culture of cyber awareness is crucial. In the Asia Pacific region, where businesses have been facing a surge in cyberattacks, fostering this awareness is more important than ever. FIs need to conduct continuous training to improve security literacy among employees, implement best practices such as software and system updates, adopt a zero-trust security model, and enforce strong password policies.

In addition to cyber hygiene and employee awareness, FIs must take a holistic view of operational resilience by implementing the following fundamental

Enhancing operational resilience in FIs **BEGINS WITH A STRONG FOUNDATION IN CYBER HYGIENE.** Implementing measures such as multi-factor authentication, proactive threat monitoring, timely vulnerability patching, and robust network security controls are essential steps. These practices not only protect critical systems but also ensure compliance with evolving regulatory frameworks across the Asia Pacific region.

principles, which can provide a starting point to build upon and customise, depending on the institution's size, complexity, and role in the wider financial services ecosystem.

1. **Assess internal and External Factors to Identify Threats**
   - **Understand your critical operations:** Identify business-critical operations and the internal and external systems and processes they depend on.
   - **Understand your risk and threat landscape:** Organisations can map out potential risks by collaborating with cybersecurity teams, information-sharing groups, and government agencies. Maintaining an updated internal inventory of physical and digital assets, threats, and types of events is also integral to effective response planning.

2. **Plan to Protect and Respond**
   - **Develop a risk-based approach to protect critical operations:** Define acceptable risk outcomes aligned with the organisation's risk appetite and set maximum tolerable levels of disruption for key operations. This enables prioritisation of mitigation efforts. One way to develop a risk-based approach is to gain access to cross-border and timely threat intelligence through trusted information-sharing communities. Staying informed about the global threat landscape enables FIs to stay ahead of cross-border threats that may migrate across markets and jurisdictions.
   - **Develop effective response plans to maintain control during crises:** Create response frameworks that clearly outline roles, responsibilities, communication paths, and escalation procedures, incorporating lessons learned from past incidents and exercises.

3. **Take Preemptive Measures**
   - **Participate in exercises:** Regularly simulate cyber incident scenarios to test internal and external response capabilities and ensure crisis protocols are practical, feasible, and up to date. This includes participating in industry-led exercises and public-private collaborative initiatives designed to safeguard the collective financial services sector. These include resilience exercises such as Locked Shields or government-led initiatives such as the Monetary Authority of Singapore and US Treasury's bilateral cybersecurity workshops.
   - **Implement effective governance:** Ensure that enterprise-wide resilience programmes comply with relevant laws, regulations, and standards, with clear oversight structures to drive continual improvement and coordinated action during disruptions.

In today's evolving threat landscape, where attackers and defenders often have access to the same tools, **FIs NEED A BROAD, MULTI-LAYERED, AND PROACTIVE RISK MANAGEMENT STRATEGY** that ensures cyber preparedness and business continuity amid increasingly complex and inevitable threats.

OPERATIONAL RESILIENCE IS THE BEST RISK MANAGEMENT STRATEGY

In today's evolving threat landscape, where attackers and defenders often have access to the same tools, FIs need a broad, multi-layered, and proactive risk management strategy that ensures cyber preparedness and business continuity amid increasingly complex and inevitable threats.

This strategy goes beyond financial recovery to safeguard operations, maintain trust, and ensure both financial and operational stability in a hostile and evolving digital landscape — where no organisation is immune to cyber risk. ✱

■ *Christophe Barel is the Managing Director for Asia Pacific at FS-ISAC, the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. Founded in 1999, the organisation's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defence.*