Opening Remarks

TB-CERT Cybersecurity Annual Conference 2026

Dr. Daranee Saeju, Assistant Governor, Bank of Thailand

Good morning,
Your Excellency Deputy Prime Minister,
Chairman of the Thai Bankers' Association,
Distinguished guests, executives, colleagues, and members of the TB-CERT community.

<u>I. Trust as the foundation of Digital Finance</u>

It is a great honor and pleasure to join you today.

In our line of work, we often see incidents as data, alerts, or case numbers. Today, I'd like to begin with a person. A retired schoolteacher. We'll call her **"Khun Kru Noi".**

One ordinary morning, while having breakfast, her phone rang. The caller introduced himself as an officer from her bank. He knew her name. He knew which bank she used. He sounded completely legitimate. He told her that her account had been used as a mule account and that he was calling to help protect her. She followed his instructions. Within minutes, her life savings disappeared.

Unfortunately, stories like this are far too common. Many of us know someone who has experienced a scam like this. Some of us may even have come close ourselves. **But this story is about much more than one victim. Behind a single phone call lies an entire criminal ecosystem—fraud, cybercrime, money laundering, and the financing of other illicit activities.**

These are not separate problems. They are different chapters of the same story. **If we are to protect people effectively, we must tackle the entire ecosystem—not just individual incidents.**

Ladies and gentlemen,

Every successful scam does more than take away someone's savings. It chips away at something even more precious—**Trust.**

Trust that our financial system is safe.
Trust that digital finance can be relied upon.
Trust that innovation is working for honest people—not for criminals.

People embraced digital banking because they trusted the safeguards we put in place. **That is why cybersecurity is not simply an IT issue. It is fundamental to preserving trust in our financial system.**

Every day, millions of people entrust us with their savings, their payments, and their financial future. **Our responsibility is to ensure that this trust is never taken for granted.** And earning that trust requires us to stay ahead of constantly evolving threats.

<u>II: Evolving Threats & Safeguarding System Integrity</u>

Over the past several years, the Bank of Thailand, together with the industry, has significantly strengthened our safeguards against fraud and scams.

We have enhanced **mobile banking security,** and I am pleased to say that, for the past one and a half years, Thailand has not recorded a single unauthorized mobile banking transaction caused by so-called "money malware".

We have also introduced more **proactive measures against digital fraud**, implemented **a shared responsibility framework**, and **strengthened supervisory expectations** across the industry. These are important steps. But we also recognize that the threat continues to evolve—and so must our response.

Cybersecurity is no longer only about protecting systems from external attacks. It is also about preventing our own financial infrastructure from being exploited for fraud, money laundering, and other illicit financial activities.

The most damaging adversary we face today does not always breach a firewall. He opens a mule account. He passes our verification. He exploits legitimate financial infrastructure to move illicit funds through networks and across borders in a matter of seconds.

This reminds us that protecting trust means more than protecting our networks. It means protecting the integrity of the financial system itself.

Our financial system exists to create opportunities for people and businesses—not opportunities for criminals.

Banks exist to help families save, businesses invest, and economies grow. They must never be used to facilitate illicit activities or become channels for criminal enterprises.

III: Responsible Innovation

Technology is transforming finance at an extraordinary pace, and artificial intelligence brings tremendous opportunities. But like **every powerful technology, its benefits come with risks.** AI gives criminals new capabilities, but it also gives us more powerful tools to protect the financial system. We can use AI to strengthen authentication, identify suspicious behavior, uncover hidden mule account networks, detect threats earlier, respond more quickly, and reduce harm when incidents occur.

Responsible innovation therefore means more than adopting new technologies. It means ensuring that every innovation is secure by design, transparent, accountable, and ultimately serves the public.

This is precisely why today's conference is so important. It is an opportunity for us to learn from one another, share experiences, challenge assumptions, and explore new ways of staying ahead of increasingly sophisticated threats. **More importantly, it reminds us that no single institution can do this alone.** By combining technology with collaboration, shared intelligence, and responsible innovation, we can, together, better protect the integrity of the financial system.

IV: Conclusion

Ladies and gentlemen,

TB-CERT plays a vital role in turning that vision into reality. It is more than a cyber response team. It is a trusted community that brings together expertise, intelligence, and actions to strengthen our collective resilience against emerging threats.

Before I close, let me return to “**Khun Kru Noi**”. Imagine a different ending. The fraudulent call is detected. The mule account is frozen. Intelligence is shared across institutions. The suspicious transaction is stopped before the money leaves the financial system. She finishes her breakfast without ever knowing she almost became a victim.

Perhaps that is the greatest measure of our success - not simply how well we respond to incidents, **but how effectively we prevent them** through intelligence sharing, collaboration and collective action, **before harm is ever done.** People often ask whether our financial system is cyber secure. That is certainly important.
But perhaps the more important question is this: Is it trust secure?

Because every scam we prevent
every mule account we freeze
every illicit transaction we intercept
every criminal network we disrupt
ultimately protects one thing. Trust.

The trust that people place in their banks.
The trust that businesses place in our financial institutions.
The trust that enables innovation to flourish.
And ultimately, the public confidence on which our financial system depends.

The ultimate objective is not simply to defend our networks. It is to preserve public confidence in our financial system.

So let us not only secure our financial system—let us strengthen the trust that sustains it.

Thank you, and I wish you all a productive and inspiring conference.