Address by Shri Tuhin Kanta Pandey, Chairman, SEBI
"SEBI Symposium on Cyber Defence"
Aug 17, 2026

Distinguished guests, international delegates, representatives of fellow financial-sector regulators, regulated entities, members of the technology and academic community,

A very warm welcome to all of you to this Symposium on Cyber Defence.

I am particularly delighted that we have also international participants from 15 jurisdictions within IOSCO joining domestic participants for this symposium. It is encouraging to see such a diverse group of jurisdictions, institutions and perspectives represented here.

This diversity is important.

The cyber resilience that we see today is the outcome of efforts across a much wider ecosystem — regulators, financial institutions, academia, technology institutions — all contributing in different ways.

I would particularly like to acknowledge the role of Rashtriya Raksha University in strengthening research, talent and specialised capabilities in cybersecurity, as well as its contribution to this programme. I would also like to thank NISM for facilitating and helping organise this symposium and for its continued contribution to capacity building in the securities-market ecosystem.

The steps taken by SEBI and fellow financial-sector regulators, along with the efforts of MIIs and regulated entities, have strengthened cybersecurity and resilience across the financial markets.

However, the cyber landscape is evolving faster than ever. The threats are becoming more interconnected and sophisticated. That is why we thought it was important to bring this entire ecosystem together not merely to discuss cybersecurity, but to build greater collective cyber resilience.

One Connected Ecosystem

On one hand, interconnectedness creates enormous efficiency. On the other hand, it also creates dependencies. A weakness at one point can have consequences far beyond that point. An incident may begin with one organisation, but the impact may travel through a vendor, a technology platform, a third party or a connected institution.

The question is no longer simply: Is my organisation secure?
The more important question is: Is the ecosystem resilient?

The World Economic Forum's Global Cybersecurity Outlook 2026 highlights that strengthening collective cyber resilience has become both an economic and a societal imperative. Cybersecurity is an area where collaboration remains not only possible, but particularly powerful.

From Cybersecurity to Cyber Resilience

So, the question before us is perhaps no longer whether a cyber-incident will happen. The more relevant question is: When it happens, how ready are we?

How quickly can we detect it?
How quickly can we contain it?
How quickly can we recover?

And perhaps most importantly — how quickly can we share what we have learnt, so that another institution does not become the next victim?

This is where cyber resilience becomes critical. Cyber resilience does not mean assuming that our systems can never be attacked. It means building the capability to **anticipate, withstand, respond to, recover from and learn** from an attack.

Every organisation should therefore have a clear incident response and recovery plan.

Not a plan that exists only in a document. A plan that has been tested. A plan in which people know their roles.

A plan that answers very practical questions: Who takes the decision when an incident occurs? Who isolates the affected system? Who communicates with the regulators and other relevant stakeholders?

And, most importantly, how do we restore critical operations safely and quickly?

It requires **leadership, preparation, coordination and clarity of responsibility.** That is why the design of this symposium is so important.

Over the next few days, you will not merely listen to lectures and presentations. You will participate in workshops and tabletop exercises. You will experience real-time scenarios through the Cyber Range. You will engage with technology providers, researchers and industry practitioners.

I would therefore encourage every participant to use this opportunity not merely to demonstrate what you already know, but to discover where your assumptions may fail under pressure.

Another important area in cybersecurity where I believe our thinking needs to change fundamentally is **vulnerability management.**

For years, it followed a predictable cycle—conduct a VAPT, identify and classify vulnerabilities, remediate them, and repeat the exercise months or even a year later. That approach is increasingly outdated.

Today, vulnerabilities, software, cloud configurations, APIs and third-party dependencies are changing continuously. With newer AI models accelerating both attacks and defence, vulnerability management too must become continuous, dynamic and risk-driven, rather than a periodic compliance exercise.

But technology alone is not the answer.

The real objective should be a continuous cycle:
Discover. Assess. Prioritise. Remediate. Validate. And repeat.

And this brings me to the closely connected issue of **patch management.**

Knowing about a vulnerability is not enough if it remains unpatched for weeks or months. We need intelligent, risk-based and increasingly automated patch management — particularly for critical vulnerabilities — with rapid deployment and verification that remediation has actually worked.

SEBI - Building Resilience for Today's Threats - and Tomorrow's

Over years SEBI has been working towards strengthening the cybersecurity posture of the securities market and has developed the Cybersecurity and Cyber Resilience Framework.

But building resilience also means preparing for risks that may not yet be fully visible today. One such area is quantum computing.

We have embedded quantum resilience as a core pillar of our cybersecurity and cyber resiliency strategy, aligned with India's National Quantum Mission (NQM).

At the global level, SEBI is serving as Vice Chair of IOSCO's FinTech Task Force (FTF) Quantum Computing Working Group (QWG) and contributing to work on assessing capacity in **quantum computing and quantum preparedness**.

Quantum computing holds enormous promise for science, technology and finance. But it may also challenge some of the cryptographic assumptions on which today's digital systems are built. And the concern is not only about the day when a sufficiently powerful quantum computer becomes available.

The concern is also about data that can be captured today and potentially decrypted in the future. That is why post-quantum cryptography cannot remain a research topic for tomorrow. It has to become a migration programme for today.

Many regulators across the world, including SEBI, have already begun encouraging organisations to transition towards quantum-safe standards and solutions.

For financial-sector organisations, this means we need to start asking practical questions.

Where are we using quantum-vulnerable cryptography? Which systems and applications depend upon it? Which vendors and third parties depend upon it? How long would it take to replace those systems?

And do we have **crypto-agility**—the ability to change cryptographic algorithms without redesigning the entire system?

We should not wait for a quantum threat to materialise before beginning the migration.

Quantum readiness is a resilience programme, not a science-fiction exercise.

At the same time, we must look forward rather than simply defend the past.

AI, agentic systems, automation, advanced analytics and eventually quantum technologies will change the way cyber defence itself is conducted.

The opportunity is to use these technologies responsibly to build systems that can identify anomalies, correlate intelligence, prioritise vulnerabilities, recommend actions and, where appropriate and properly governed, initiate defensive responses.

But as we introduce more autonomy, we also introduce new risks. Therefore, AI for cybersecurity must itself be secure, governed and accountable.

From Individual Defence to Collective Defence

This brings me to perhaps the most important message I would like to leave with all of you.

Cybersecurity is no longer only an IT issue.
It is a board-level issue.
It is a business-continuity issue.

It is a market-integrity issue.
It is an investor-confidence issue.

Cyber threats do not respect organisational boundaries. They do not respect regulatory boundaries. And they certainly do not respect national borders.

Our response cannot stop at those boundaries either. If one institution learns from an attack, that learning should help protect others.

If one regulator develops a good practice, it should become a reference point for others. If one country develops a successful capability, there should be channels through which others can learn from it. In cyberspace, our collective resilience depends on the strength of the connections between us.

This is also the thinking behind the initiatives we have launched today.

The revamped **SEBI Incident Reporting Portal** is designed to make reporting more structured, timely and actionable, while aligning with the FSB FIRE (Format for Incident Reporting Exchange). This will facilitate greater uniformity and reduce friction in cross-border incident reporting.

Another initiative — **Cyber Suraksha Portal** — is intended to create a central hub for sharing cybersecurity knowledge, vulnerability warnings, policy measures and incident insights across the securities-market ecosystem.

These are not merely technology platforms. Their real value will come from the knowledge they enable us to share and the action that knowledge enables us to take.

Making This Symposium a Beginning, Not an Event

I hope this symposium becomes a place where we exchange more than presentations.

Let us exchange experiences.
Let us share difficult lessons.
Let us discuss what did not work.
Let us challenge conventional thinking.
Let us understand new technologies.

And let us build relationships that remain useful long after this symposium concludes. I would particularly encourage candid feedback. Tell us what worked. Tell us what did not.

Our objective should be very simple: Every participant should leave this symposium better prepared than when they arrived.

Take back not just presentations or certificate. Take back a new idea, a new capability, a new connection — something that strengthens your organisation's preparedness.

Conclusion

Let me conclude with three words: Cooperate. Prepare. Respond.

Cooperate — because cyber threats are borderless.
Prepare — because resilience is built before an incident, not during it. And,
Respond — because when an incident occurs, speed, coordination and decisive action matter.

The threat landscape will continue to evolve.
AI will evolve. Attack techniques will evolve. Technology will evolve.

Our cyber defence must therefore evolve faster. Let this symposium be a commitment to that evolution. A commitment to continuous learning. A commitment to stronger capabilities. And above all, a commitment to collective cyber resilience.

I once again warmly welcome all our domestic and international participants.

I wish you productive discussions, challenging simulations, new partnerships and, most importantly, practical learning that strengthens our collective financial ecosystem.

I wish you all a very successful Symposium on Cyber Defence.

Thank You.