Title : The Future of Cybersecurity: Threats, Challenges, and Innovations

Date **:** 5 Juni 2025

Venue **:** Online

Sector **:** All Sector

Speaker **:**

1. **Paul Rafiuly**
   Direktur Technology & Operations, UOB Indonesia
2. **Bryan Tan**
   a partner in the firm’s Entertainment & Media Group Singapore
3. **Alfons Tanujaya**
   Pakar Cybersecurity dan Ketua Komtap Cyber Security Awareness

Background :

- Di tengah perkembangan era digital yang begitu pesat, sektor keuangan menjadi salah satu sektor yang menghadapi lonjakan ancaman siber yang semakin kompleks dan canggih. Berdasarkan proyeksi Cybersecurity Ventures, kerugian global akibat kejahatan siber diperkirakan mencapai USD 10,5 triliun pada tahun 2025, meningkat dari USD 9,5 triliun pada 2024. Proyeksi ini mencerminkan eskalasi signifikan baik dari sisi frekuensi maupun dampak serangan siber di tingkat global.
- Ancaman siber tidak hanya semakin sering terjadi, namun juga semakin sulit dideteksi seiring dengan pemanfaatan teknologi canggih seperti kecerdasan buatan (AI), *machine learning*, dan komputasi kuantum. Ransomware, malware, serta serangan berbasis *social engineering* seperti phishing masih menjadi jenis ancaman yang paling dominan. Data menunjukkan bahwa serangan ransomware meningkat hingga 81% dari tahun 2023 ke 2024, sementara *phishing* mengalami kenaikan sebesar 58,2% sepanjang tahun 2023, dengan sektor keuangan sebagai salah satu target utama.
- Kemunculan teknologi *deepfake* yang semakin marak juga menambah kompleksitas lanskap ancaman. Sejak tahun 2019, insiden terkait *deepfake* telah meningkat sebesar 550%, dan diperkirakan akan mencapai angka 8 juta pada tahun 2025. Teknologi ini banyak disalahgunakan untuk tujuan manipulasi informasi dan penipuan digital berskala besar. Lebih dari itu, sekitar 40% dari insiden siber saat ini diketahui melibatkan pemanfaatan AI, menjadikan serangan semakin canggih dan sulit diantisipasi. Di sisi lain, pemanfaatan AI untuk tujuan pertahanan siber juga terus berkembang, meskipun masih menghadapi tantangan implementasi. Hanya 37% organisasi yang telah memiliki mekanisme evaluasi keamanan sebelum mengadopsi solusi berbasis AI, meskipun 66% mengakui bahwa AI merupakan *game-changer* dalam strategi keamanan siber.
- Tantangan lainnya mencakup meningkatnya kerentanan dalam rantai pasok digital, belum selarasnya regulasi antar yurisdiksi, serta keterbatasan talenta siber yang juga perlu mendapatkan perhatian. Menanggapi dinamika tersebut, inovasi dan kolaborasi lintas sektor menjadi aspek yang sangat krusial. Pendekatan seperti arsitektur *Zero Trust*, segmentasi mikro, enkripsi secara *real-time*, serta otomatisasi pada Security Operations Center (SOC) menjadi tren utama dalam memperkuat ketahanan siber di tahun 2025. Namun, efektivitas pendekatan tersebut sangat bergantung pada dukungan regulasi yang kuat serta pengembangan kapasitas sumber daya manusia yang adaptif terhadap perubahan lanskap ancaman.
- Merespon isu ini, OJK Institute menginisiasi penyelenggaraan webinar yang diharapkan menjadi ruang diskusi yang konstruktif untuk membahas lanskap ancaman siber beserta trend terkini, mengidentifikasi tantangan dalam implementasi kebijakan keamanan digital, serta menggali strategi dan inovasi mitigasi risiko guna memperkuat ketahanan siber di sektor jasa keuangan Indonesia.

Objective	:	1. Meningkatkan pemahaman terkait trend ancaman dan *cyber security* terkini di tingkat global dan nasional. 2. Meningkatkan pemahaman terkait pentingnya *cyber security* pada sektor keuangan di tengah akselerasi transformasi digital. 3. Mengidentifikasi tantangan dan peluang yang terkait dengan ancaman keamanan siber dan kesenjangan ekosistem digital dalam industri jasa keuangan di Indonesia. 4. Memperkuat kolaborasi antara regulator, penyedia layanan keuangan, dan *stakeholder* terkait.
Participant	:	Pimpinan dan Pegawai OJK, Perwakilan Industri Jasa Keuangan, Akademisi dan Masyarakat Umum
Partner	:	