RISIKO OPERASI

Institusi kewangan kekal berdaya tahan dari segi operasi dan terus memperkukuh ketersediaan mereka terhadap risiko siber

Institusi kewangan secara relatif pantas membuat penyesuaian terhadap sekatan pergerakan yang lebih ketat pada separuh pertama tahun 2021, berdasarkan pengalaman terdahulu dalam menguruskan cabaran operasi sejak bermulanya pandemik. Tiada gangguan utama operasi dicatatkan pada peringkat sistem keseluruhan, dengan kerugian risiko operasi menurun sebanyak 18.7% kepada RM118.1 juta berbanding dengan separuh pertama tahun 2020. Walau bagaimanapun, institusi kewangan terus meningkatkan tahap kewaspadaan terhadap potensi risiko gangguan teknologi maklumat (*information technology*, IT) dan serangan siber. Keupayaan pengesanan dan pemulihan yang lebih kukuh yang dibangunkan oleh institusi kewangan telah berjaya mencegah sebarang gangguan pada peringkat seluruh sistem yang disebabkan oleh IT dan insiden siber pada tempoh tersebut. Institusi kewangan juga telah memperkukuh kawalan terhadap projek-projek penambahbaikan IT bagi meminimumkan kegagalan IT akibat ralat pemprosesan. Yang penting, usaha berterusan untuk mempertingkatkan dan mengekalkan amalan baik keselamatan siber (*cyber hygiene*) terus menjadi keutamaan. Penambahbaikan berterusan terhadap pelan kesinambungan perniagaan (*business continuity plan*, BCP) dan pelan pemulihan bencana (*disaster recovery plan*, DRP) institusi kewangan dengan mengambil kira pengaturan kerja jarak jauh juga telah meningkatkan kesiapsiagaan institusi kewangan dalam menghadapi krisis.

Pelbagai kerjasama yang dilaksanakan pada peringkat industri, negara dan serantau terus menyokong keupayaan sektor kewangan untuk mengesan dan bertindak balas dengan pantas terhadap ancaman siber, lantas memastikan penyediaan perkhidmatan kewangan penting tidak terganggu (Gambar Rajah 1.2). Pengaturan ini telah ditingkatkan lagi apabila Platform Risikan Ancaman Siber Sektor Kewangan (Financial Sector Cyber Threat Intelligence Platform, FinTIP)[40] mula beroperasi pada bulan September 2021. Keahlian Kumpulan Kerja Siber (Cyber Working Group, CWG) yang ditubuhkan oleh Bank juga telah berkembang untuk merangkumi dua institusi kewangan tambahan pada tahun 2021, menjadikan jumlahnya sebanyak 11 ahli. CWG terus memainkan peranan aktif dalam memastikan proses komunikasi berjalan dengan lancar dan pantas antara ahli mengenai ancaman siber yang baru timbul serta interaksi dan perbincangan mengenai inisiatif untuk mengekalkan tahap ketersediaan pertahanan siber yang kukuh. Pada peringkat serantau, Bank terus memanfaatkan Cybersecurity Resilience and Information Sharing Platform (CRISP) untuk bertukar-tukar maklumat dalam kalangan bank-bank pusat ASEAN.

Serangan perisian tebusan (*ransomware*) dan kelemahan penyedia perkhidmatan pihak ketiga (*third party service provider*, TPSP) telah menjadi tumpuan utama dalam pengukuhan dasar dalaman institusi kewangan, dan juga merupakan sumber risiko yang telah mendapat perhatian Bank. Dalam beberapa bulan kebelakangan ini, serangan perisian tebusan yang berlaku sekali-sekala menyebabkan beberapa gangguan kepada operasi perniagaan dua institusi kewangan, namun serangan tersebut dapat dibendung dengan berkesan. Risiko yang berkaitan dengan penggunaan TPSP juga telah meningkat dengan ketara bagi sesetengah institusi kewangan yang sangat bergantung pada perkhidmatan pihak ketiga akibat pelarasan operasi yang dibuat sebagai tindak balas kepada pandemik. Risiko ini termasuklah TPSP yang mungkin tidak dapat memenuhi perjanjian tahap perkhidmatan (*service level agreement*) disebabkan oleh sekatan operasi yang dikenakan di bawah perintah kawalan pergerakan yang dilanjutkan; infrastruktur IT TPSP yang tidak dilindungi secukupnya daripada kegagalan IT dan ancaman siber; serta BCP dan DRP TPSP yang lemah dan boleh menghalang keupayaan mereka untuk menyokong institusi kewangan secara berkesan semasa krisis.

Pihak Bank sedang memantau dengan teliti langkah-langkah yang diambil oleh institusi kewangan untuk menguruskan risiko-risiko ini. Institusi kewangan telah mempergiat usaha untuk mengkaji semula secara berkala kawalan risiko dan kemampanan kewangan TPSP bagi memastikan kesinambungan perkhidmatan. Langkah-langkah ini termasuk

[40] Rujuk Rencana Maklumat 'Pembentukan Platform Risikan Ancaman Siber Sektor Kewangan (FinTIP)' untuk maklumat lanjut mengenai FinTIP.

Gambar Rajah 1.2: Pengaturan Industri untuk Menyokong Pengesanan dan Tindak Balas Terhadap Ancaman Siber



Sumber: Bank Negara Malaysia

melakukan kajian semula yang khusus terhadap BCP TPSP. Beberapa institusi kewangan juga telah menambah baik struktur fi yang terikat dengan perjanjian tahap perkhidmatan untuk menyelaraskan dengan lebih baik kawalan risiko dan kualiti perkhidmatan yang disampaikan oleh TPSP. Institusi kewangan juga sedang memperkukuh strategi tindak balas mereka untuk menguruskan potensi gangguan kepada perkhidmatan TPSP dengan mengambil kira ketiadaan perkhidmatan TPSP secara tiba-tiba sebagai sebahagian daripada ujian BCP dan pelan kontingensi institusi kewangan itu sendiri.

Tumpuan institusi kewangan pada TPSP tertentu, dan risiko penularan yang berkaitan dengan kesalinghubungan antara TPSP dengan sistem kewangan boleh menimbulkan risiko sistemik. Memandangkan lebih banyak perkhidmatan yang sedang beralih kepada platform digital yang disokong oleh pihak ketiga, terdapat keperluan untuk memastikan risiko tersebut dapat dikenal pasti dan dimaklumkan dengan lebih berkesan pada peringkat institusi dan sistem. Perkara ini memerlukan institusi kewangan membuat padanan kesalinghubungan mereka secara menyeluruh dengan penyedia perkhidmatan dalam seluruh rantaian nilai (secara fizikal dan secara maya). Hal ini bertujuan untuk mengenal pasti dan memantau risiko tumpuan dan penularan. Seterusnya, langkah ini boleh dibangunkan untuk membentuk peta penularan siber (*cyber contagion map*) pada peringkat seluruh sistem bagi memberikan gambaran agregat mengenai kesalingbergantungan dan kesalinghubungan yang berkaitan antara komponen IT asas, TPSP yang menyokong sistem kewangan, dan rangkaian kewangan. Dapatan daripada penilaian ini dijangka dapat memberikan lebih banyak maklumat untuk latihan simulasi krisis, pengurangan risiko dan pelaksanaan BCP sektor kewangan pada masa hadapan.

Semenjak pengaturan kerja yang fleksibel dan dari jarak jauh menjadi kelaziman, Bank juga telah meningkatkan tumpuannya terhadap kecukupan kawalan institusi kewangan. Tindakan ini bertujuan

melindungi data sulit memandangkan penggunaan platform dan peranti yang tidak dilindungi boleh menimbulkan risiko keselamatan IT yang ketara ketika menjalankan tugas harian. Secara amnya, syarat untuk mengakses data sulit dan aplikasi kritikal secara jarak jauh terus menjadi salah satu pertimbangan keselamatan yang utama. Bagi kebanyakan institusi kewangan, akses sedemikian tertakluk pada takrifan keadaan yang terhad dengan perlindungan keselamatan siber yang telah dipertingkatkan. Misalnya, hampir kesemua institusi kewangan telah menggunakan alat pencegahan kehilangan data, mewujudkan tindak balas dan strategi pemulihan yang jelas untuk mengehadkan kesan sebarang pencerobohan data, dan menguatkuasakan akses pengguna yang terhad kepada data sulit. Institusi kewangan dikehendaki menilai semula kecukupan kawalan ini secara berterusan sejajar dengan prospek untuk mengekalkan pengaturan kerja yang fleksibel dan dari jarak jauh untuk tempoh yang lebih lama daripada jangkaan, atau menerapkan perubahan yang kekal dalam operasi perniagaan mereka akibat pandemik.

Sistem pembayaran dan penyelesaian terus berdaya tahan dari segi operasi

Kedua-dua Sistem Pemindahan Dana dan Sekuriti secara Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities System, RENTAS)[41] dan sistem pembayaran runcit (*retail payment systems*, RPS) terus mengekalkan ketersediaan sistem yang tinggi, tanpa sebarang insiden atau gangguan besar terhadap perkhidmatan. Langkah-langkah BCP yang mantap seperti pembahagian operasi, tahap lewahan (*redundancy*) yang tinggi, dan pasukan sandaran telah menyokong kelancaran operasi sistem pembayaran. Bank juga membuat penilaian terhadap RPS yang mendorong pengendali sistem pembayaran bertindak bagi mengukuhkan lagi langkah kawalan yang akan meningkatkan daya tahan siber RPS. Perkara ini termasuklah langkah-langkah meningkatkan sumber khusus untuk menguruskan operasi keselamatan siber, memperkukuh sistem pemantauan dan kawalan, dan meningkatkan teknik dan metodologi ujian keselamatan. Pelancaran jalinan pembayaran QR dengan PromptPay[42] pada bulan Jun 2021 membolehkan pembayaran kod QR rentas sempadan secara masa nyata dilaksanakan di Malaysia dan Thailand. Langkah pengurusan risiko yang teguh juga diselaraskan antara Bank dengan Bank of Thailand bagi memastikan rangkaian pembayaran rentas sempadan yang kukuh dan selamat.

Memandangkan urus niaga pembayaran masa nyata terus berkembang dengan pantas, risiko kredit dan penyelesaian yang berkaitan dengan beberapa RPS yang diselesaikan atas dasar penyelesaian bersih tertunda (*deferred net settlement*, DNS) telah meningkat. Bagi melindungi institusi kewangan daripada risiko penyelesaian, Payments Network Malaysia Sdn Bhd (PayNet) sedang berusaha untuk menyediakan pengaturan pencagaran (*collateralisation arrangements*) untuk DNS pada Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payments Platform, RPP), Bursa Pemprosesan Kewangan (Financial Process Exchange, FPX), MyDebit dan Rangkaian ATM Bersama (Shared ATM Network, SAN) menjelang akhir tahun 2021. Di bawah pengaturan tersebut, peserta dalam sistem ini dikehendaki memperuntukkan wang tunai dan/atau sekuriti sebagai cagaran bagi memenuhi obligasi penyelesaian mereka.

Pada 1 Julai 2021, Bank telah mengambil alih operasi RENTAS daripada PayNet sebagai sebahagian daripada rancangan untuk mengukuhkan lagi pengurusan risiko RENTAS secara menyeluruh. Pemindahan tersebut diselesaikan dengan lancar tanpa gangguan operasi. Pemindahan ini akan mengurangkan risiko integrasi dan penyelarasan antara Bank dengan PayNet kerana Bank kini akan memiliki, mengendali dan menyediakan sokongan teknologi dan infrastruktur kepada sistem itu. Sejajar dengan amalan terbaik antarabangsa, pengaturan tadbir urus yang jelas dan telus telah dikekalkan susulan pemindahan tersebut. Yang nyata, tanggungjawab Bank untuk pengawasan dan pengawalseliaan terhadap infrastruktur pasaran kewangan utama, termasuk RENTAS, dan peranannya sebagai pengendali RENTAS juga akan terus diasingkan dengan jelas dalam struktur organisasi Bank. Satu jawatankuasa pengurusan khusus juga telah ditubuhkan untuk menyelia operasi, pembangunan dan pengurusan risiko RENTAS. Jawatankuasa ini termasuk empat wakil luar yang mempunyai pengalaman dan kepakaran yang berkaitan dalam bidang IT serta teknologi kewangan (*financial technology*, FinTech) dan ekosistem pembayaran.

[41] RENTAS ialah sistem penyelesaian kasar masa nyata untuk pemindahan dana antara bank, penyelesaian sekuriti hutang dan perkhidmatan penyimpanan untuk sekuriti hutang tanpa skrip.

[42] PromptPay merupakan sistem pembayaran runcit masa nyata di Thailand yang memudahkan pembayaran dan pemindahan dana melalui saluran elektronik (contohnya, perbankan internet, perbankan mudah alih dan ATM).

Pembentukan Platform Risikan Ancaman Siber Sektor Kewangan (FinTIP)

Serangan siber boleh menimbulkan risiko yang besar terhadap kestabilan kewangan dengan industri kewangan dijangka menghadapi peningkatan ancaman dari segi kekerapan, kecanggihan dan skop. Perkembangan ini bukan hanya berlaku di Malaysia. Pada peringkat global, terdapat peningkatan jumlah serangan siber yang telah menjejaskan operasi perniagaan utama. Yang penting, sebahagiannya dirancang oleh pelaku ancaman menggunakan taktik canggih untuk mengeksploitasi bilangan laluan masuk (*entry points*) rangkaian dan sistem institusi kewangan. Hal ini berlaku disebabkan oleh penerapan sistem yang boleh diakses melalui Internet (*Internet-facing*) serta pendigitalan perkhidmatan kewangan yang pesat. Pelaku ancaman ini beroperasi dalam ekosistem rahsia yang aktif untuk berkongsi maklumat, menyelaraskan serangan, merekrut penggodam, menjual data yang dicuri (*compromised data*) dan menyediakan perkhidmatan jenayah siber.

Peningkatan jumlah serangan tersebut dan sifatnya yang cukup tersusun memerlukan tindak balas sektor kewangan yang terselaras. Institusi kewangan terus membuat pelaburan besar bagi menyediakan perlindungan IT dan daya tahan siber dalam institusi masing-masing. Namun, satu strategi pihak berkepentingan berbilang dalam seluruh industri untuk mempertahankan sistem kewangan daripada ancaman siber yang lazim diperlukan bagi memperkukuh usaha setiap institusi kewangan. Bagi tujuan ini, Bank telah berusaha mewujudkan platform risikan dan kerjasama ancaman siber untuk industri kewangan. Platform Risikan Ancaman Siber Sektor Kewangan (Financial Sector Cyber Threat Intelligence Platform), atau FinTIP, mula beroperasi pada bulan September 2021.

FinTIP akan memperkukuh kerjasama industri dan menggalakkan perkongsian maklumat

FinTIP bertujuan untuk mencapai tiga matlamat utama:

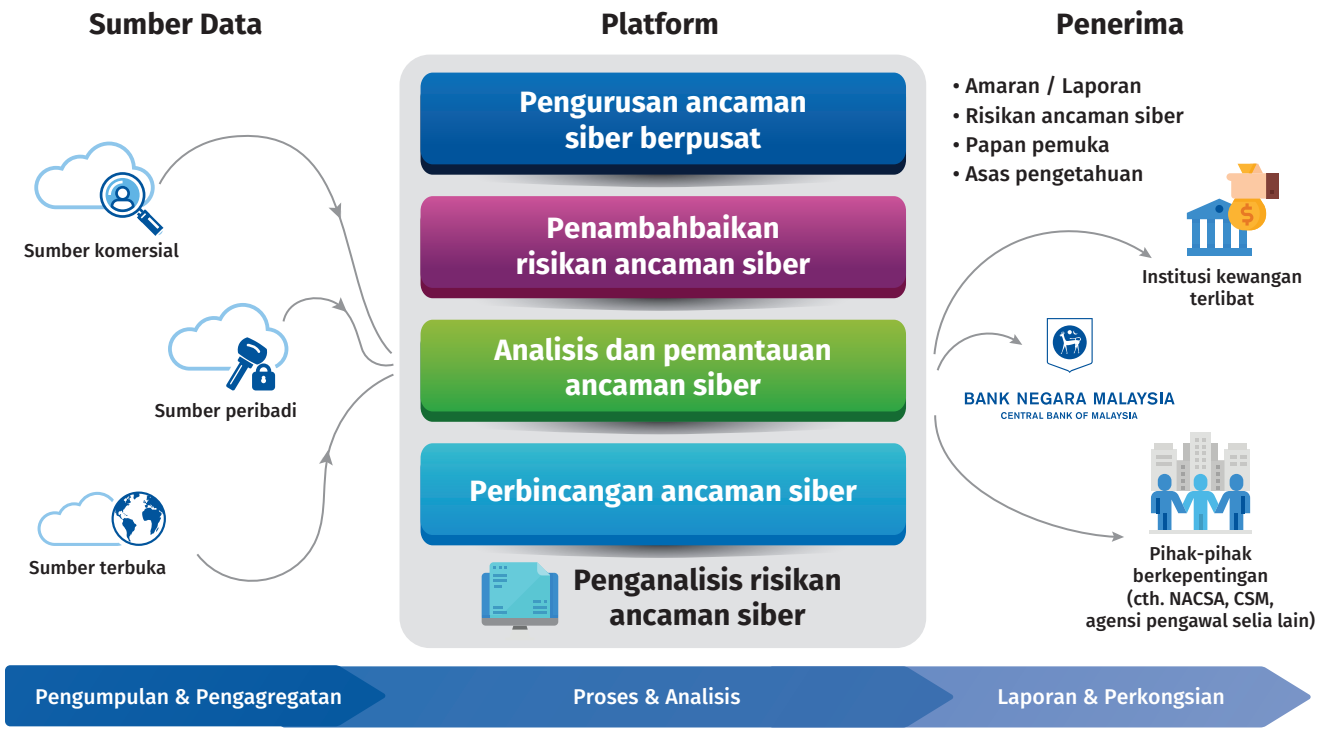
- Melaksanakan penilaian dan penyebaran maklumat secara pantas mengenai ancaman siber yang muncul dan kelemahan IT yang kritikal;
- Menggalakkan perkongsian maklumat dan kerjasama merentas industri melalui platform yang selamat dan dipercayai; dan
- Meningkatkan kesedaran situasi siber bagi membantu proses membuat keputusan yang strategik.

Pelaksanaan FinTIP oleh Bank dapat membantu membina kepercayaan, sekali gus mengurangkan halangan utama terhadap perkongsian maklumat dan kerjasama yang meluas antara institusi kewangan dengan pihak berkepentingan utama yang lain. Pihak berkepentingan dalam sektor awam dan swasta boleh mengambil bahagian dan memberikan sumbangan kepada FinTIP dengan berkongsi maklumat secara sulit mengenai ancaman siber, insiden dan kelemahan IT pada masa hampir nyata (*near real-time*). Pada peringkat kebangsaan, FinTIP berfungsi untuk menghubungkan dan memudahkan pertukaran maklumat rentas sektor antara sektor kewangan dengan sektor ekonomi yang lain, melalui entiti seperti Agensi Keselamatan Siber Kebangsaan (National Cyber Security Agency, NACSA), CyberSecurity Malaysia (CSM), Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dan Suruhanjaya Sekuriti Malaysia.

Penilaian dan penyebaran maklumat yang pantas

FinTIP, yang beroperasi secara 24x7x365, akan mengumpulkan, menggabungkan dan menganalisis risikan ancaman siber dan kelemahan IT daripada pelbagai sumber, serta menyebarkan maklumat yang relevan kepada pihak berkepentingan tepat pada masanya (Gambar Rajah 1.3). Platform analisis ini memanfaatkan gabungan algoritma mesin dan kepakaran manusia untuk menghubungkaitkan, menyelaraskan, memperkaya, dan memurnikan data terkumpul untuk menghasilkan risikan yang boleh diambil tindakan pada masa nyata. Institusi kewangan boleh menggunakan maklumat yang disediakan oleh FinTIP untuk tindak balas insiden, operasi keselamatan, pemburuan ancaman, pengurusan kelemahan dan analisis risiko mereka sendiri. Mereka juga boleh mendapatkan perkhidmatan profesional untuk bantuan mengenai pemulihan insiden siber dan analisis ancaman. Gambar Rajah 1.4 menerangkan ciri-ciri penting FinTIP.

Gambar Rajah 1.3: Model Penggunaan FinTIP



Sumber: Bank Negara Malaysia

Gambar Rajah 1.4: Ciri-Ciri FinTIP

Pemantauan landskap ancaman berterusan

Papan pemuka masa nyata – papan pemuka yang boleh diubah suai terdiri daripada pelbagai jenis data dan rajah.

Tahap dedahan – hubungkan inventori aset yang dihantar dengan kelemahan yang diketahui pada masa nyata.

Penanda aras rakan setara – tahap prestasi atau tahap dedahan institusi kewangan ditanda aras dengan rakan setara dalam industri.

Laporan landskap ancaman – muat turun laporan landskap ancaman berkala dengan mudah secara terus daripada portal FinTIP.

Komunikasi dan penyebaran kepada industri

Penyebaran amaran dan khidmat nasihat tepat pada masanya kepada pihak yang berkaitan.

Saluran perbincangan yang dipercayai – untuk memudahkan perkongsian maklumat dan kerjasama dalam organisasi dan industri.

Analisis menyeluruh oleh penganalisis ancaman siber

Analisis perisian hasad dan *shellcode* – permohonan analisis terperinci untuk mengenal pasti dan memahami tingkah laku kod yang mungkin berbahaya dengan memuat naik artifak ke FinTIP.

Sandbox – buka dan uji program atau fail yang tidak dipercayai melalui sandbox FinTIP (persekitaran yang selamat).

Perkongsian risikan ancaman siber setempat

Perkongsian risikan setempat yang selamat – sumber risikan peribadi yang dimuat naik ke FinTIP akan dikumpulkan, dilaraskan dan dibuang identiti sebelum dikongsikan dengan lebih banyak pihak.

Sumber: Bank Negara Malaysia

Meningkatkan kerjasama industri

FinTIP juga menyediakan platform yang selamat kepada institusi kewangan dan pihak berkepentingan lain merentas industri untuk bertukar-tukar maklumat mengenai langkah-langkah bertahan yang diambil dan iktibar yang dipelajari daripada insiden siber. Sebagai contoh, institusi kewangan boleh mengambil bahagian dalam perbincangan yang diadakan oleh komuniti untuk bekerjasama dan saling belajar daripada pengalaman masing-masing dalam menangani ancaman lazim. Institusi kewangan juga dapat memperoleh pemahaman yang objektif mengenai prestasi risiko siber atau tahap dedahan mereka, yang ditanda aras berdasarkan rakan setara dalam industri.

Meningkatkan kesedaran situasi siber

FinTIP meningkatkan kesedaran situasi siber industri secara keseluruhan dengan memberikan pandangan yang lebih holistik mengenai pelaku ancaman yang menjadikan industri tempatan sebagai sasaran serta membantu institusi kewangan memahami dengan lebih baik tentang taktik, teknik dan prosedur pelaku ancaman. Data terkumpul mengenai ancaman dan kelemahan IT dipadankan dengan aset IT yang digunakan dalam industri untuk memberikan maklumat yang tepat tentang tahap dedahan siber tempatan. Maklumat ini akan membolehkan Bank mengenal pasti kelemahan khusus dan menilai potensi kesan ancaman siber kepada seluruh sistem.

Laporan yang dihasilkan oleh FinTIP bersifat taktikal, operasi dan strategik untuk memenuhi keperluan khalayak yang pelbagai. Pada peringkat taktikal, laporan teknikal memberikan data terperinci mengenai penunjuk ancaman siber yang dapat disepadukan oleh institusi kewangan dalam instrumen keselamatan siber mereka bagi mengenal pasti dan mengurangkan ancaman siber. Pada peringkat operasi, institusi kewangan akan dapat menjejak kempen serangan dan melakukan pemprofilan pelaku ancaman untuk mendapatkan pemahaman yang lebih baik mengenai pelaku ancaman yang menjadikan institusi kewangan sebagai sasaran. Hal ini akan membolehkan institusi kewangan memberikan keutamaan dan melaksanakan operasi keselamatan siber yang lebih bersasar. Akhir sekali, pada peringkat strategik, institusi kewangan boleh menggunakan data FinTIP untuk membuat keputusan perniagaan yang bijak dengan lebih memahami cara peristiwa global dan tempatan, serta landskap ancaman yang berubah-ubah dapat mempengaruhi tahap ketersediaan keselamatan siber sesebuah institusi kewangan.

FinTIP melengkapi strategi pertahanan pelbagai lapisan sedia ada

FinTIP mencerminkan perkongsian tanggungjawab untuk keselamatan siber dengan memudahkan pendekatan seluruh industri ke arah meningkatkan daya tahan siber. Penting dinyatakan bahawa FinTIP berfungsi untuk melengkapi dan menambah, dan bukannya menggantikan, perkhidmatan risikan ancaman siber sedia ada dalam institusi itu sendiri. Bank menjangkakan FinTIP akan menyokong perkongsian maklumat dan kerjasama secara lebih mendalam dan lebih pantas yang seterusnya memperkukuh keupayaan tindak balas industri kewangan terhadap ancaman siber yang berubah-ubah dan menjejaskan sistem kewangan.