OPERATIONAL RISK

Financial institutions remained operationally resilient and continue to strengthen their cyber security risk posture

Financial institutions adapted relatively quickly to the stricter movement restrictions in the first half of 2021, leveraging earlier experience in managing operational challenges since the onset of the pandemic. No major operational disruptions were recorded at the system-wide level, with operational risk losses declining by 18.7% to RM118.1 million compared to the first half of 2020. Financial institutions, however, remained highly vigilant of potential risks from information technology (IT) disruptions and cyber-attacks. Stronger detective and recovery capabilities developed by financial institutions have prevented any system-wide disruptions caused by IT and cyber incidents encountered during the period. Financial institutions have also further strengthened controls around IT enhancement projects to minimise IT failures caused by processing errors. Critically, ongoing initiatives to improve and maintain good cyber hygiene practices continue to be a high priority. Ongoing enhancements to financial institutions' business continuity plans (BCPs) and disaster recovery plans (DRPs) to reflect remote working arrangements have also led to further improvements in financial institutions' crisis preparedness.

The various collaborative arrangements in place at the industry, national and regional levels continue to support the financial sector's ability to swiftly detect and respond to cyber threats, thus ensuring the uninterrupted provision of essential financial services (Diagram 1.2). These arrangements were further enhanced with the operationalisation of the Financial Sector Cyber Threat Intelligence Platform (FinTIP)[40] in September 2021. Membership of the Cyber Working Group (CWG) established by the Bank has also expanded to include two additional financial institutions in 2021, resulting in a total of 11 members. The CWG continues to play an active role in facilitating swift communications between members on emerging cyber threats and engagements on initiatives to maintain a strong cyber defence posture. At the regional level, the Bank continues to leverage the Cybersecurity Resilience and Information Sharing Platform (CRISP) to exchange information among ASEAN central banks.

Diagram 1.2: Industry Arrangements to Support Detection and Responses to Cyber Threats

Deployment of Financial Sector Cyber Threat Intelligence Platform (FinTIP)

01 FinTIP is an industry platform that collects, aggregates and analyses cyber threat data in real time from various sources. FinTIP facilitates the sharing of information to the Bank and participating financial institutions to ensure rapid identification and detection of emerging cyber threats and critical IT vulnerabilities.

02 FinTIP will also foster industry collaboration and cooperation, serving as a platform for community-driven discussions on cyber threats.

Implementation of Cyber Incident Scoring System (CISS)

01 Financial institutions are required to immediately report any cyber incidents to the Bank using the CISS template, which comprises six key pieces of information. The Bank should also be promptly updated as new information becomes available.

02 The Bank will assess the severity and determine the potential systemic impact of the incident.

03 Actionable cyber threat intelligence will be disseminated to the industry in a timely manner so that appropriate prevention, detection and response measures can be implemented.

Regular engagements with various stakeholders

01 The Bank has established the Cyber Working Group which comprises selected financial institutions that meet quarterly to discuss emerging cyber risks in the industry.

02 The Bank also regularly engages agencies such as National Cyber Security Agency (NACSA), CyberSecurity Malaysia, Securities Commission Malaysia and Malaysia Communication & Multimedia Commission (MCMC) to share cyber information and coordinate responses to cyber threats.

Establishment of Cybersecurity Resilience and Information Sharing Platform (CRISP)

01 CRISP is a regional platform for ASEAN central banks to share each country's cyber threat landscape and intelligence, facilitate discussions on emerging cyber risks, and support capacity building of cyber risk specialists and supervisors.

Source: Bank Negara Malaysia

[40] Refer to the Information Box on 'Establishment of the Financial Sector Cyber Threat Intelligence Platform (FinTIP)' for further details on FinTIP.

Ransomware attacks and vulnerabilities within third party service providers (TPSPs) have been a key focus of strengthened internal policies of financial institutions, and are also sources of risk that the Bank is focused on. In recent months, sporadic ransomware attacks caused some disruptions to the business operations of two financial institutions, but they were effectively contained. Risks associated with the use of TPSPs have also increased substantially for some financial institutions that have relied more heavily on third party services as a result of operational adjustments made in response to the pandemic. These risks include TPSPs that may be unable to meet service level agreements due to operational restrictions imposed under extended movement control orders; IT infrastructure of TPSPs that are inadequately protected against IT failures and cyber threats; and weak BCP and DRP of TPSPs that may hamper their ability to effectively support financial institutions during a crisis.

The Bank is closely monitoring measures by financial institutions to manage these risks. Financial institutions have intensified periodic reviews of the risk controls and financial sustainability of TPSPs to ensure the continuity of services rendered. This includes specific reviews of the BCPs of TPSPs. Some financial institutions have also enhanced the fee structures that are tied to service level agreements to better align risk controls and the quality of services delivered by TPSPs. Financial institutions are also strengthening their response strategies to manage potential disruptions to TPSP services by including the sudden unavailability of TPSPs as part of financial institutions' own BCP tests and contingency plans.

The concentration of financial institutions to specific TPSPs, and contagion risks associated with interlinkages between TPSPs and the financial system, could pose systemic risks. With more services moving onto digital platforms supported by third parties, there is a need to improve visibility over such risks at both the institution and system levels. This will require financial institutions to comprehensively map their interlinkages with service providers across the value chain (both physically and virtually) in order to identify and monitor concentration and contagion risks. This in turn can be developed into a cyber contagion map at the system-wide level to provide an aggregate view of the relevant interdependencies and interconnections between underlying IT components, TPSPs that support the financial system, and the financial network. Results from these assessments are expected to better inform crisis simulation exercises, risk mitigations and BCPs for the financial sector going forward.

As remote and flexible working arrangements become the norm, the Bank has also increased its focus on the adequacy of controls by financial institutions to protect confidential data given that the use of unsecured platforms and devices to perform day-to-day tasks poses significant IT security risks. In general, conditions for remote access to confidential data and critical applications continue to be one of the key security considerations, and for many financial institutions, such access is limited to narrowly defined circumstances with enhanced cyber security safeguards. For example, almost all financial institutions have deployed data loss prevention tools, established clearly defined response and recovery strategies to limit the impact of any data breach, and enforced restricted user access to confidential data. Financial institutions are expected to continuously re-evaluate the adequacy of these controls in line with prospects of keeping remote and flexible working arrangements in place for longer than expected, or adopting permanent changes in their business operations as a result of the pandemic.

Payment and settlement systems continued to be operationally resilient

Both the Real-time Electronic Transfer of Funds and Securities System (RENTAS)[41] and retail payment systems (RPS) continued to maintain high system availability, with no major incidents or service disruptions. Robust BCP measures such as split operations, high level of redundancy, and reserve teams supported the smooth operations of the payment systems. The Bank also conducted an assessment on RPS which led to actions by payment system operators to further strengthen control measures that will increase the cyber resilience of RPS. These include measures to increase dedicated resources to manage cyber security operations, strengthen monitoring and control systems, and enhance security testing techniques and

[41] RENTAS is a real-time gross settlement system for interbank fund transfers, debt securities settlement and depository services for scripless debt securities.

methodologies. With the launch in June 2021 of a QR payment linkage with PromptPay[42] that enables instant cross-border QR code payments in Malaysia and Thailand, robust risk management measures were also jointly coordinated between the Bank and Bank of Thailand (BOT) to ensure a strong and secure cross-border payment network.

As real-time payment transactions continued to grow at an accelerated pace, the associated credit and settlement risks in several RPS that are settled on a deferred net settlement (DNS) basis have increased. To safeguard financial institutions against settlement risks, the Payments Network Malaysia Sdn Bhd (PayNet) is working to put in place collateralisation arrangements for DNS on the Real-time Retail Payments Platform (RPP), Financial Process Exchange (FPX), MyDebit and Shared ATM Network (SAN) by end-2021. Under the arrangements, participants in these systems will be required to set aside cash and/or securities as collateral to meet their settlement obligations.

On 1 July 2021, the Bank assumed operations of RENTAS from PayNet as part of plans to further strengthen the end-to-end risk management of RENTAS. The transfer was completed smoothly with no operational disruptions. This transfer will reduce integration and coordination risks between the Bank and PayNet as the Bank will now own, operate and provide the technology and infrastructure support to the system. In line with international best practices, clear and transparent governance arrangements have been preserved following the transfer. Notably, the Bank's responsibilities for the regulatory and supervisory oversight of key financial market infrastructures, including RENTAS, and its role as the operator of RENTAS, will continue to be clearly segregated within the Bank. A dedicated management committee has also been established to oversee the operations, development, and risk management of RENTAS. The committee includes four external representatives with relevant experience and expertise in IT as well as the financial technology (FinTech) and payments ecosystem.

[42] PromptPay is a real-time retail payment system in Thailand that facilitates payments and fund transfers via electronic channels (e.g. internet banking, mobile banking and ATMs).

Establishment of the Financial Sector Cyber Threat Intelligence Platform (FinTIP)

Cyber-attacks can pose considerable risks to financial stability with the financial industry expected to face threats that are growing in frequency, sophistication and scope. This development is not unique to Malaysia. Globally, there has been an increasing number of cyber-attacks that have brought down key business operations. Of note, some of these were orchestrated by threat actors using highly sophisticated tactics which exploit the higher number of entry points into the network and systems of financial institutions as a result of the rapid adoption of Internet-facing systems and greater digitalisation of financial services. These threat actors operate in an active underground ecosystem where they share information, coordinate attacks, recruit hackers, sell compromised data and provide cybercrime services.

The increased intensity of such attacks and their well-coordinated nature call for a coordinated financial sector response. While financial institutions have continued to invest extensively in IT hardening and cyber resilience in their respective institutions, an industry-wide, multi-stakeholder strategy to defend the financial system against common cyber threats is needed to reinforce the efforts of individual financial institutions. To this end, the Bank has been working to establish a cyber threat intelligence and collaboration platform for the financial industry. The Financial Sector Cyber Threat Intelligence Platform, or FinTIP, commenced operations in September 2021.

FinTIP to strengthen industry collaboration and foster information sharing

The FinTIP is intended to achieve three key goals:

- Perform rapid assessment and dissemination of information on emerging cyber threats and critical IT vulnerabilities;
- Foster information sharing and collaboration across the industry via a secured and trusted platform; and
- Increase cyber situational awareness to aid strategic decision-making.

The operation of FinTIP by the Bank helps to build trust, thereby reducing a key barrier to widespread information sharing and collaboration between financial institutions and other key stakeholders. Stakeholders in public and private sectors can participate and contribute to FinTIP by confidentially sharing information on cyber threats, incidents and IT vulnerabilities in near real-time. At the national level, FinTIP serves as a bridge to connect and facilitate cross-sector information exchange between the financial sector and other economic sectors via entities such as the National Cyber Security Agency (NACSA), CyberSecurity Malaysia (CSM), Malaysian Communication and Multimedia Commission (MCMC) and Securities Commission Malaysia (SC).

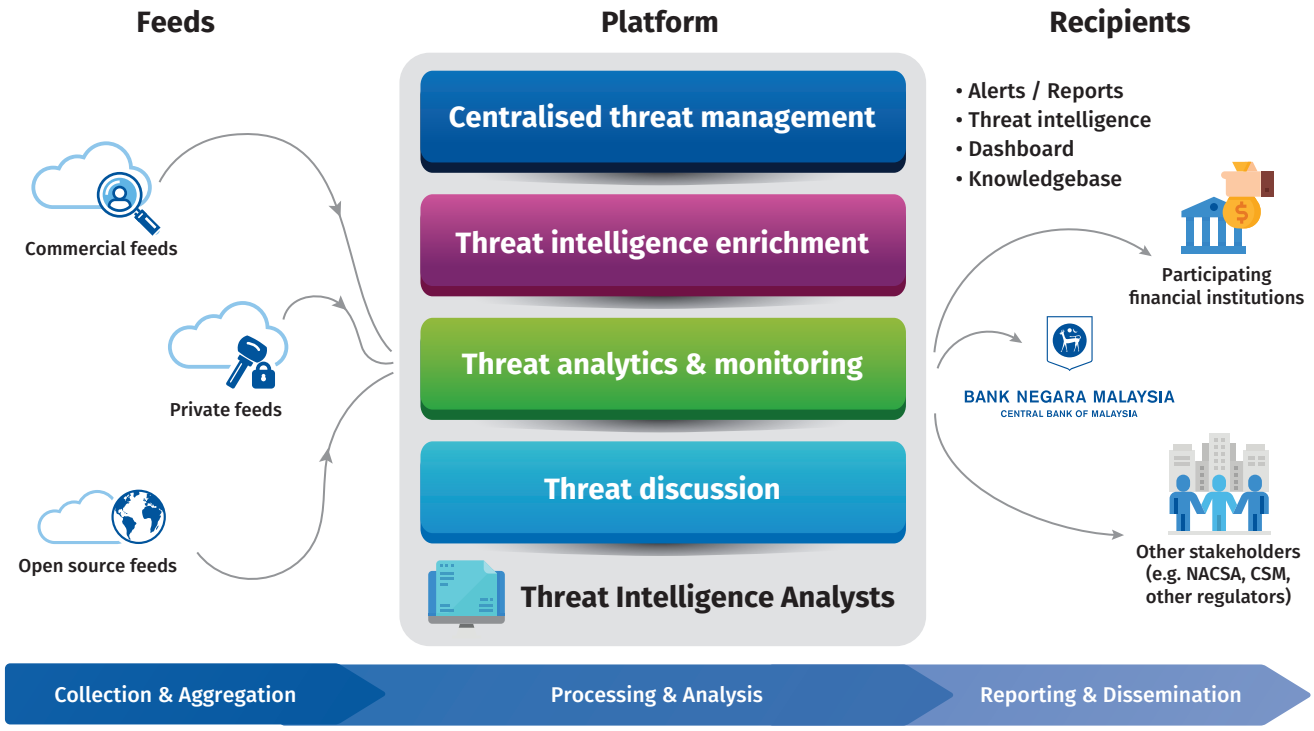
Rapid information assessment and dissemination

FinTIP, which operates on a 24x7x365 basis, will collect, aggregate and analyse cyber threat intelligence and IT vulnerabilities from various sources, and distribute relevant information to stakeholders in a timely manner (Diagram 1.3). This analytical platform leverages a combination of machine algorithms and human experts to correlate, normalise, enrich, and sanitise collected data to produce real-time actionable intelligence. Financial institutions can use the information provided by FinTIP for their own incident response, security operations, threat hunting, vulnerability management and risk analysis. They can also access professional services for assistance on cyber incident remediation and analysis of threats. Diagram 1.4 describes the key features of FinTIP.

Improving industry collaboration

FinTIP also provides a secure platform for financial institutions and other stakeholders across the industry to exchange information on defensive measures taken and lessons learnt from cyber incidents. For example, financial institutions can participate in community-driven discussions to collaborate and learn from each other's experiences in dealing with common threats. Financial institutions can also obtain an objective understanding of their cyber risk performance or exposure level, benchmarked against industry peers.

Diagram 1.3: FinTIP Deployment Model



Source: Bank Negara Malaysia

Diagram 1.4: FinTIP Features

Continuous threat landscape monitoring

Real-time dashboard – personalised dashboard consisting of representation of different data types, sightings and charts.

Exposure level – correlate submitted asset inventory against known vulnerabilities in real-time.

Peer benchmarking – measure performance or exposure level against the aggregated industry level.

Threat landscape reports – easily export periodic threat landscape report directly from FinTIP portal.

Industry broadcast & communication

Timely dissemination – of alerts and advisories to the relevant parties.

Trusted discussion channel – to facilitate information exchange and collaboration within the organisation and within the industry.

Advanced analysis by threat analysts

Malware and shellcode analysis – request in-depth analysis to understand the behaviour of potentially malicious code by submitting artefacts to FinTIP.

Sandboxing – execute untrusted programs or files via FinTIP's sandbox (safe environment).

Localised threat intelligence sharing

Secure local intelligence sharing – private intelligence feed submitted into FinTIP will be collected, sanitised and even anonymised before being shared to the wider audience.

Source: Bank Negara Malaysia

Enhancing cyber situational awareness

FinTIP increases overall industry cyber situational awareness by providing a more holistic view of threat actors targeting the local industry and helps financial institutions better understand the threat actors' tactics, techniques, and procedures. Data collected on threats and IT vulnerabilities are mapped to the IT assets used within the industry to provide an accurate localised cyber exposure level. This information will enable the Bank to pinpoint specific vulnerabilities and assess the potential system-wide impact of a cyber threat.

The reports produced by FinTIP are tactical, operational and strategic in nature to cater for a diverse audience. At the tactical level, technical reports provide granular data on cyber threat indicators which financial institutions can integrate into their cyber security tools to identify and mitigate cyber threats. At the operational level, financial institutions will be able to track attack campaigns and undertake actor profiling to gain a better understanding of the threat actors that target the financial institution. This will enable financial institutions to prioritise and perform more targeted cyber security operations. Finally, at the strategic level, financial institutions can use FinTIP data to inform business decisions by better understanding how global and local events, and the evolving threat landscape affect a financial institution's cyber security posture.

FinTIP complements existing multi-layered defence strategies

FinTIP reflects a shared responsibility for cyber security by facilitating a whole-of-industry approach towards enhancing cyber resilience. It is important to note that FinTIP serves to complement and augment, rather than replace, an individual institution's own existing cyber threat intelligence services. The Bank expects FinTIP to support deeper and faster information sharing and collaboration which in turn, will strengthen the financial industry's response capabilities to the evolving cyber threats affecting the financial system.