Issue No. 1
November 2019

Regtech Watch is a newsletter published by the Hong Kong Monetary Authority to promote the use of Regtech by the banking industry. It provides information on actual or potential Regtech use cases rolled out or being explored in Hong Kong or elsewhere. The objective is to assist authorized institutions (AIs) in adopting innovative technology to enhance their risk management and regulatory compliance.

Background

Recognising the growing importance of Regtech, the HKMA has launched a series of initiatives under the Banking Made Easy initiative to facilitate the adoption of Regtech in Hong Kong. A workstream has been established to reach out to AIs, technology firms and consulting firms to understand latest initiatives and ideas in the Regtech space. Over twenty pilot trials of Regtech use cases including remote onboarding technologies have been allowed under the HKMA's Fintech Supervisory Sandbox, and around seventy discussion sessions have since been held through the Fintech Supervisory Chatroom.

In the process, the HKMA has picked up a broad range of local and overseas Regtech use cases on prudential risk management and regulatory compliance. The HKMA believes that it would be helpful to share these observations with the banking industry, through this newsletter, so as to promote the use of Regtech in Hong Kong. This inaugural issue of the Regtech Watch outlines Regtech use cases in the area of cyber defence.

It should be noted that the sole purpose of this newsletter is to provide AIs with information on latest Regtech development. The HKMA does not endorse any use cases or solutions described in this newsletter. If an AI intends to adopt a particular Regtech, it should undertake its own due diligence to ensure that the technology is suitable for its circumstances.

The HKMA welcomes any feedback or suggestions on how this newsletter can be improved to serve its purpose.

Regtech for cyber risk management

Key risk management challenges

In recent years, the increasing sophistication of cyberattacks has increased the possibility of more severe consequences such as significant disruptions to banking services, massive leakage of sensitive data or even corruption of critical data. The modality of some cyberattacks has also rendered some of the traditional cyber monitoring and detective measures (such as those relying on rule-based analysis) less effective, creating the need for more advanced capability to identify and analyse potential cyberattack attempts (through analysis of behavioural patterns) in a timely manner.

Exhibit 1: Typical sources of cyber threats

Note: As cyber threats are rapidly evolving, AIs should assess cyber threats specific to their situation on an ongoing basis

As banks continue digitalising their banking services while fraudsters use more automation in making attempts of cyberattacks, the banking industry needs to analyse enormous amount of data of their systems and networks as well as business activities and transactions in order to identify potential cyberattacks and suspicious activities.

How can Regtech help?

Given these challenges, a number of banks have started to adopt Regtech such as artificial intelligence solutions to develop insights into the multitude of behavioural information such as trends and patterns observed from system-to-system communications and from human interactions with applications. With a deeper understanding of the system or human behaviours that are considered normal, there is a better chance that anomalous activities can be identified in a timely manner. Further, Regtech solutions using behaviour-aware technologies can be used to automate day-to-day but important cyber risk management tasks to reduce human errors.

Regtech use cases

It is observed that the application of Regtech for cyber risk management is gaining popularity across banks in Hong Kong. Three examples of such use cases are summarised in the boxes below for reference.

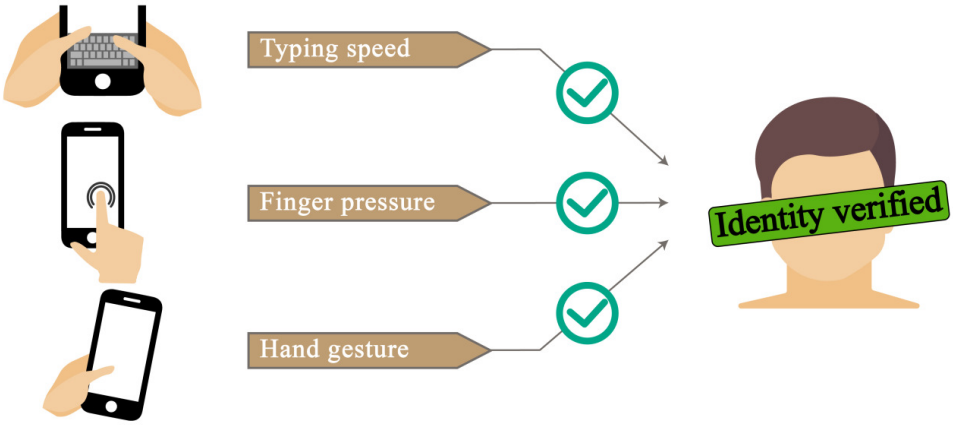
Use case 1 – Behavioural biometric techniques

User authentication has long been a fundamental control in cyber risk management. Multi-factors authentication (MFA) has also been widely implemented in the banking industry, particularly for the execution of high-risk transactions. The three types of factors used in MFA include (i) *something a customer knows*, e.g. password; (ii) *something a customer has*, e.g. security token; and (iii) *something a customer is*, e.g. fingerprint.

In a Regtech use case, "behavioural biometric techniques" have been adopted to step up user authentication and fraud detection. Specifically, these techniques are embedded in the analysis of a user's behavioural patterns such as typing speed, finger positions/pressure and even how the user holds his or her mobile device. Since these biometric data are unique to individuals, a unique identity profile can be built by applying artificial intelligence techniques to analyse the dynamic biometric data collected. The unique identity profile evolves based on the user's behaviours and thus is difficult to be copied or reproduced, especially when multiple behavioural features are examined in combination.

Such a unique identity profile not only serves as a factor of MFA (i.e. something a customer is), but also augments existing authentication approach by enabling frictionless and continuous authentication to detect anomalies (e.g. a user's identity can be transparently verified throughout an e-banking session). By the same token, behavioural biometric techniques can also be used to combat automated credential stuffing attacks, as it could be more challenging for automated robots to simulate natural human behaviours.

Exhibit 2: Illustration of behavioural biometric



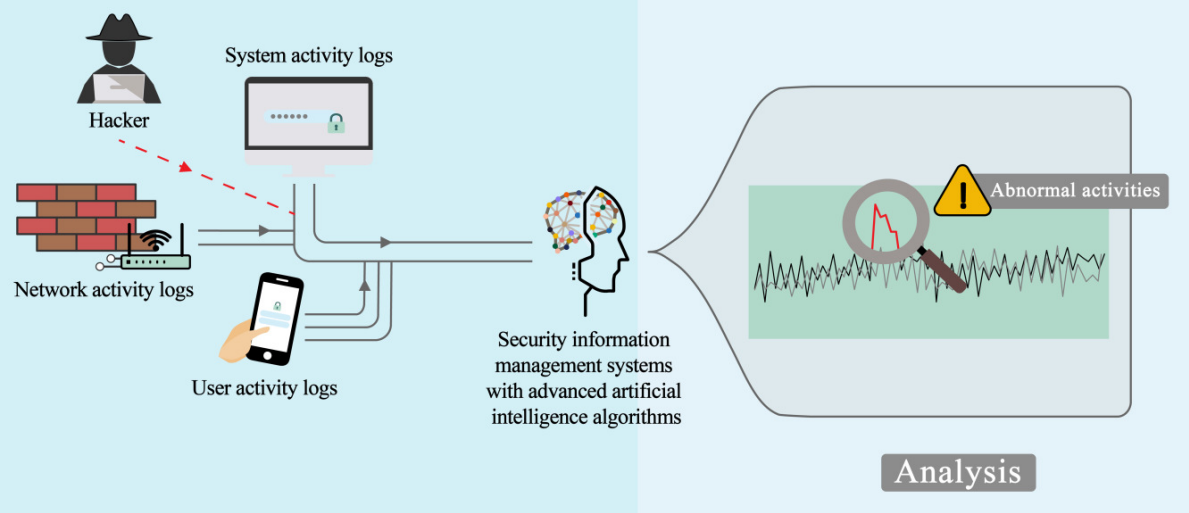
Use case 2 – Analytics of activity logs

To identify abnormal network, system and user activities, banks need to review and analyse a large volume of activity logs on a continuous basis. One typical approach is to analyse activity logs with the support of security information management systems that detect abnormal activities based on rules derived from previously known cyberattacks. One limitation of this approach is related to the inability to detect emerging cyberattacks that have not been covered by the prevailing rules. Also, this approach is typically more prone to false alarms, which will divert cybersecurity resources from more important matters.

In response to these challenges, some banks have started to explore the use of advanced artificial intelligence algorithms to continuously comprehend what normal system, network and user activities should look like, taking into account the evolving business and system environment, and then use it as a basis to detect potentially abnormal patterns. Such a holistic understanding of a large system environment, which was impossible without the assistance of

technology, provides banks with enhanced anomaly detection capability even for unseen cyberattacks. These solutions may also reduce the extent of human workload required to operate these solutions.

Exhibit 3: Artificial intelligence for analysing activity logs

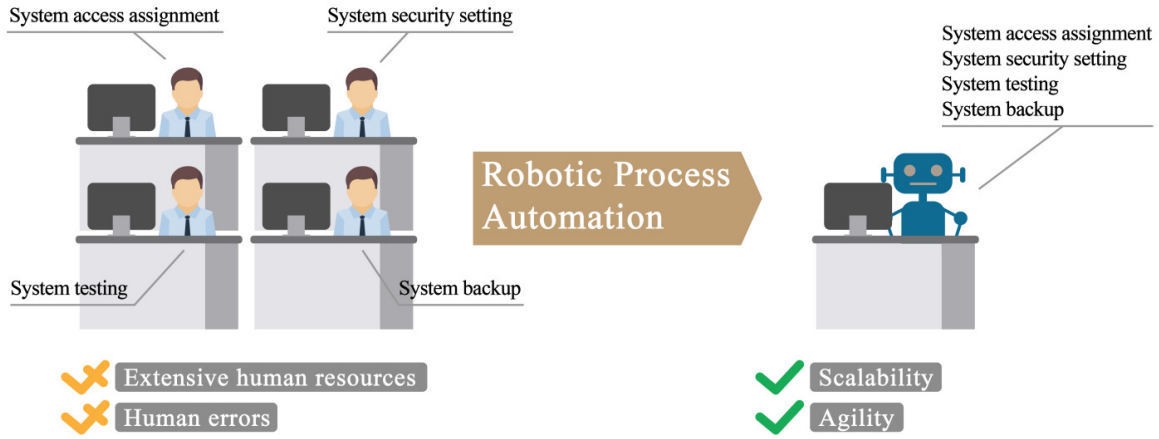


Use case 3 – Automation of cybersecurity routine tasks

In everyday cybersecurity risk management practices, extensive human resources are typically required to handle different manual tasks, such as system access assignment, system security setting and security testing.

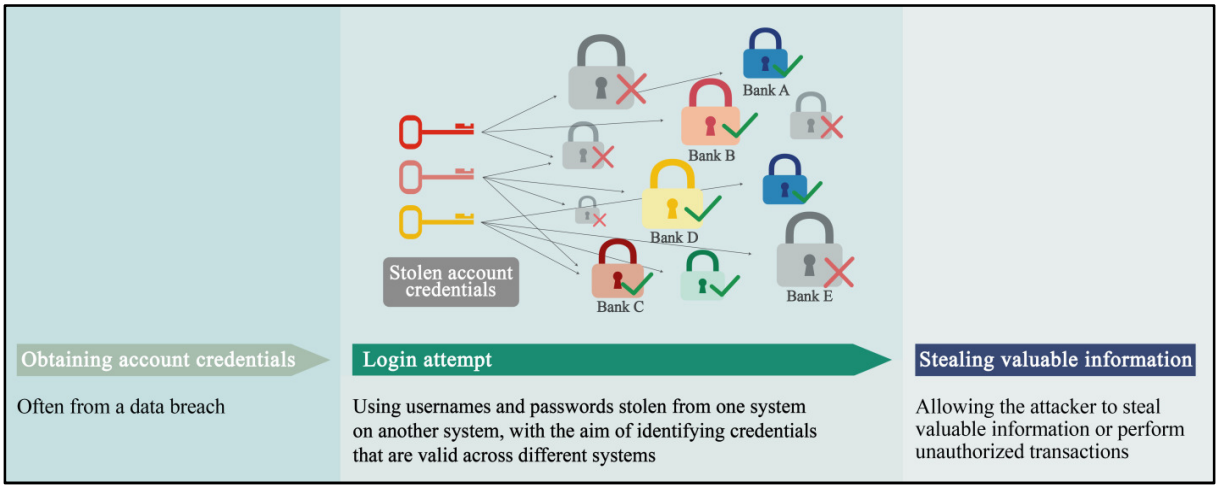
Therefore, human errors can hardly be eliminated in cyber defence even with a robust governance framework, clear operational guidelines and quality assurance efforts. In view of this, some banks are exploring the use of Robotic Process Automation (RPA), an emerging workflow automation technology. In particular, RPA makes use of software robots to observe and learn from standard users' behaviours such as how users interact with systems and how users respond to different business inputs/scenarios. Based on the behaviours learned, these software robots can automate business processes more intelligently and at a lower cost. The adoption of RPA not only helps the banks reduce human errors in cybersecurity tasks, but also increases the scalability and agility of the banks' cyber risk functions despite the scarcity of cyber expertise in the market. Banks can then focus their cybersecurity resources on more complex risk management tasks.

Exhibit 4: Robotic process automation



Apart from the above use cases, the HKMA has also noted some emerging Regtech solutions that may also be relevant to banks' cyber defence going forward. For example, there are solutions designed to deter credential stuffing attack (i.e. using usernames and passwords stolen from one system on another system, with the aim of identifying credentials that are valid across different systems). These solutions aim at tactfully replying the attackers with fake web pages so as to deceive the attackers into believing that the stolen credentials are valid, thereby reducing the value of these stolen credentials in the dark market.

Exhibit 5: Typical credential stuffing attacks



This newsletter is benefited by input and ideas contributed by the following companies:
- Blue Prism Limited
- Industrial and Commercial Bank of China (Asia) Limited
- KPMG