Trends in biometrics – Are you ready to manage cybersecurity and privacy risks?

Background

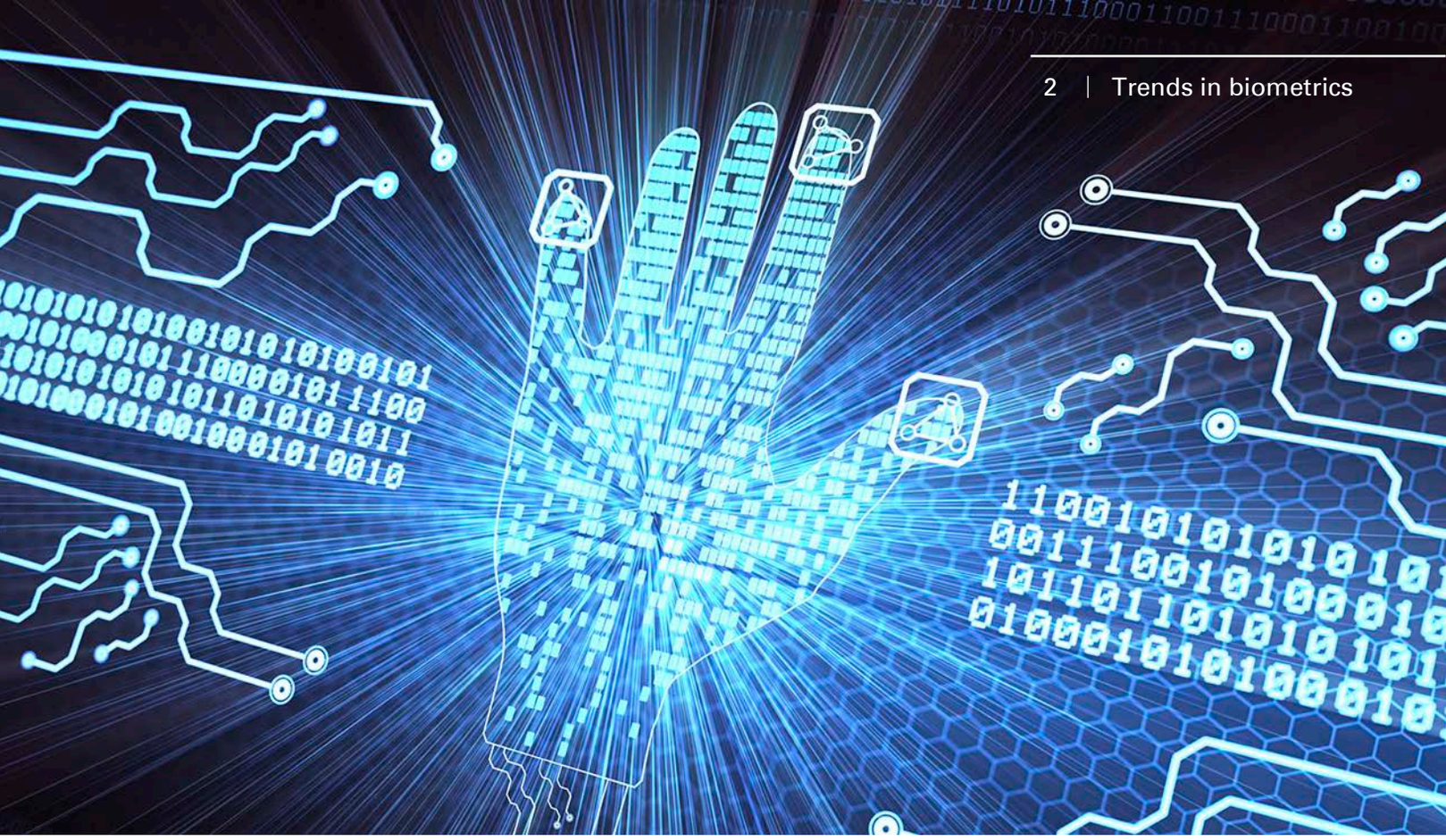
Traditional 'identity verification' often utilises user IDs and passwords. In some cases, these are combined with a hardware device (e.g. a security token) that helps provide more secure authentication.

However, in today's fast-paced world, companies need to provide convenient service and a smooth user experience to retain and engage their customers. This is one reason biometric authentication has started to gain popularity in the financial industry.

Biometric authentication refers to the use of biological characteristics for identification and authentication purposes. This means you can now rely on physical characteristics (e.g. your fingerprints), instead of on extra devices. This can markedly improve the user experience. Many companies globally, including financial institutions, are looking very closely at opportunities to implement biometric authentication in their digital operations (e.g. mobile banking and phone banking).

Is your company ready to take on cybersecurity and privacy challenges while leveraging the full potential of biometric authentication?

The three authentication factors	Examples
Something you have	Security token, ID card, mobile phone for SMS one-time password
Something you know	Password, passphrase, secret question and answer
Something you are	Biometrics



Types of biometrics in the market

The following table summarises the different types of popular biometrics:

Characteristics	Principle
Physical characteristics	Biometrics based on a person's static characteristics: Examples include fingerprints, facial features, irises and vein patterns. This biometric recognition is usually performed on a one-off basis.
Behavioural characteristics	Biometrics based on human activities, including keystroke dynamics, voice patterns, signature dynamics and gestures: Some of this authentication can be carried out on an ongoing basis.

How biometrics can be used

One advantage of using biometrics is that it is intuitive and convenient for users. For example, banks in some countries are using fingerprints for customer authentication when they use ATM machines, which saves customers the trouble of bringing an ATM card. Another example is when users are performing time-sensitive activities (e.g. authorising high-risk fund transfers or stock trading transactions). Biometrics can be used as an additional authentication factor since it saves the time of having to input extra passwords, while providing a similar level of security as extra passwords if implemented correctly.

In addition, the introduction of behavioural biometrics has also enabled an additional channel for surveillance monitoring. Abrupt deviations from the usual activities/practices can be captured via behavioural biometrics. Further analysis or investigation can then be performed to ascertain whether it is a fraud case.

Challenges to using biometrics

Despite the advantages of using biometrics, there are a number of concerns when adopting them in business operations:

Accuracy
Although biometrics mostly relates to people's physical characteristics, there is no guarantee these will remain 100% unchanged over time, which can affect the accuracy of biometrics. The effectiveness of scanners used for capturing these characteristics can also affect accuracy. The balance between accuracy and security determines the efficiency of business operations.

Security
Similar to other information captured from your customer, biometric information can be stolen. For example, fingerprints can be sampled from items that target users have touched. Those samples can then be used to recreate fingerprints, which can potentially fool fingerprint recognition systems. Biometric samples can also be obtained from compromised biometric databases if organisations have not implemented their biometric systems securely.

Regulations
Requirements from regulators and the biometric operation model will directly affect the possibility of deploying biometrics into business and the corresponding management framework required.

Irreplaceability
Unlike passwords or security devices, biometrics cannot be easily replaced. With reference to the example above, once the users' fingerprints have been compromised, it is impossible to physically replace their fingerprints, and an alternative solution has to be used to replace fingerprint authentication.

Elements of biometric governance structure

Apart from the technical infrastructure supporting the use of biometrics, a proper governance structure is crucial to the management and operation of relevant processes. The major elements of such governance structure are summarised as follows:

Privacy management

- Since the use of biometrics can be privacy-invasive by nature, privacy management is particularly important. Measures should be taken to ensure biometric data will only be used for the intended authentication purpose, and users have provided the necessary consent before the use of biometrics.

Data security management

- Data being collected when using biometrics constitutes sensitive personal data. Therefore, effective data security management programmes should be developed to ensure the relevant data is securely protected.

Compliance management

- When designing the use of biometrics, organisations should consider various compliance requirements from regulators. In particular, the Privacy Commissioner for Personal Data (PCPD) has issued a guidance note to assist companies in complying with the Personal Data (Privacy) Ordinance when using biometric data. In the financial services sector, consideration should also be given to requirements issued by the regulators to ensure the introduction of biometrics complies with the relevant requirements.

Vulnerability management

- Since biometrics information cannot be easily replaced once it has been compromised, organisations should be prepared to handle vulnerabilities or incidents related to the underlying biometric technologies deployed. They should gather the relevant intelligence, and ensure that an incident response mechanism is in place.

How can KPMG help?

KPMG China has experience providing consultancy services to help position clients for success, from strategy to operations. We have worked closely with our clients to understand their needs, and deliver cybersecurity- and privacy-related consultancy services.

Our well-developed methodologies that can address your needs include:

Governance structure design and implementation	Feasibility study	Privacy impact assessment	Compliance assessment
• Cover areas such as privacy, data security, vulnerability and compliance management in the overall governance design • Assist in implementing the governance structure and ongoing monitoring procedures	• Evaluate the pros and cons of using biometrics in business operations • Assist management in making well-informed decisions	• Evaluate the use of biometrics in terms of the impact on personal data privacy • Provide practical recommendations to mitigate identified privacy risks	• Identify possible compliance issues when deploying the use of biometrics by assessing against regulatory requirements

Contact us

Henry Shek
Partner
IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Kelvin Leung
Director
IT Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com

Alvin Li
Associate Director
IT Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Matrix Chau
Associate Director
IT Advisory
KPMG China
T: +852 2685 7521
E: matrix.chau@kpmg.com

kpmg.com/cn