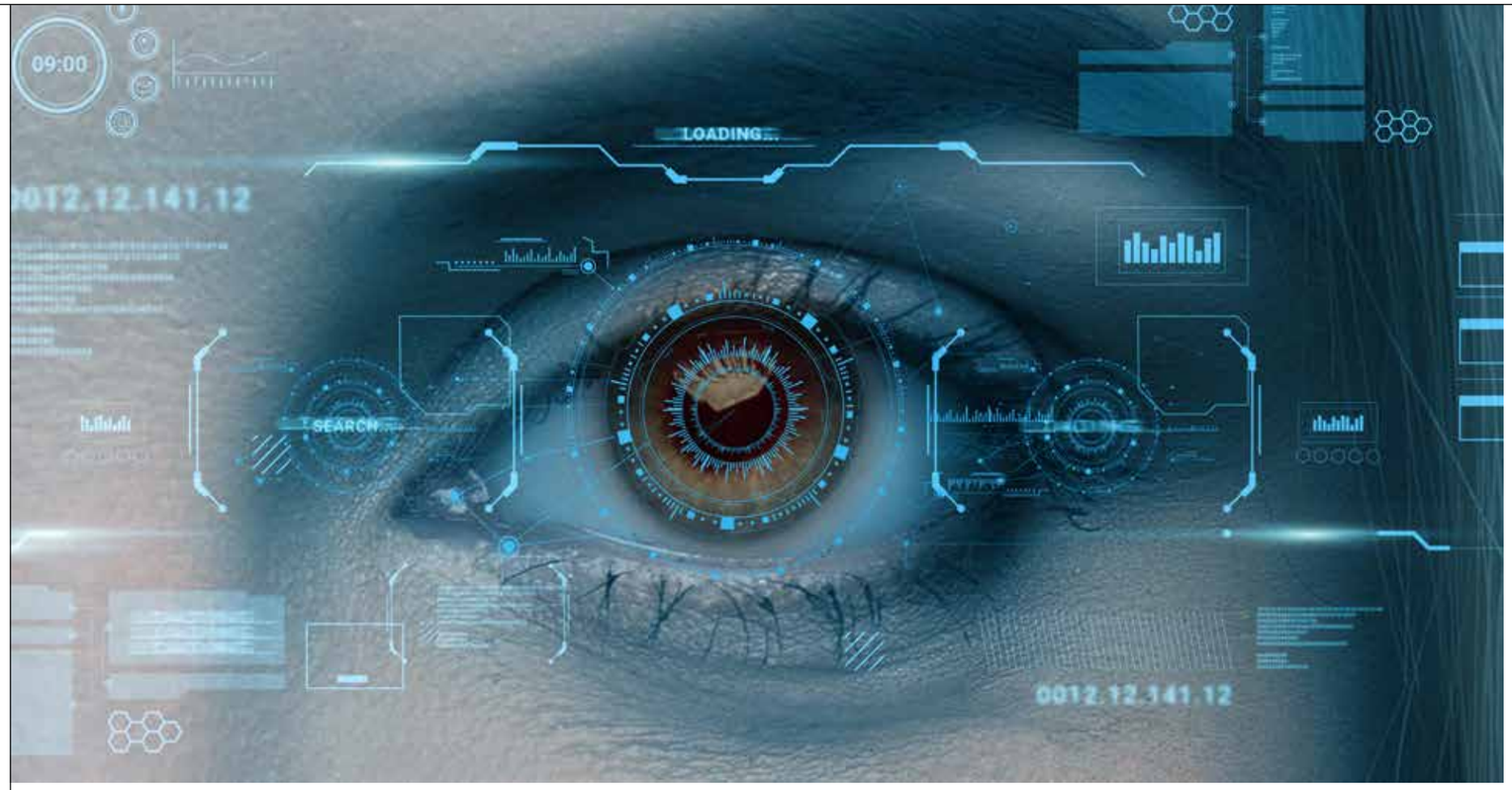

Picture credit: Adobestock

STAYING IN CHARGE

Thomas Decker *reveals why empowering individuals to control their biometric data is the new challenge across all sectors*

What if your face, fingerprint, or iris was your greatest vulnerability in a cyber attack? These unique and deeply personal identifiers are now embedded into the fabric of our daily lives. Whether for unlocking smartphones, verifying identities at workplaces or passing through airport security, biometrics promise convenience and enhanced protection. By removing the need for passwords or PIN codes, they reduce friction in authentication processes and provide seamless user experience. This widespread adoption has led to biometrics being integrated into an increasing number of critical systems, including financial services, healthcare and even national security infrastructure.

But beneath this convenience lies an unsettling question: where is this sensitive data stored, how is it used and who truly controls it? Unlike passwords that can be reset if compromised, biometric data is immutable – once stolen, it remains vulnerable indefinitely. This raises significant concerns about long-term security and data ownership, particularly as biometric authentication is increasingly used as a primary security measure across multiple sectors. Additionally, the lack of universal data protection standards means that storage practices vary widely, with some companies retaining biometric information in centralised databases, while others opt for local storage solutions embedded in personal devices.

Cyber criminals are still increasingly targeting these data sources, exploiting vulnerabilities to compromise the security and integrity of our identities. Breaches of biometric databases pose an even greater threat than traditional credential leaks because the stolen information cannot be modified. Cyber attacks targeting biometric authentication have included spoofing techniques, AI-driven Deep Fake attacks and sensor tampering, allowing hackers to manipulate or forge biometric credentials. As more industries integrate biometric authentication into critical operations, the potential consequences of a breach – ranging from financial fraud to identity theft – grow exponentially.

Biometric authentication is increasingly used as a primary security measure across multiple sectors

Industries must collaborate to rethink biometric security on a global scale, especially when it applies to high-demanding safety infrastructures. A fragmented approach to biometric security leaves gaps that cyber criminals can exploit, making cross-industry cooperation and regulatory alignment essential. Solutions such as strong encryption, decentralised data storage and continuous system updates are necessary to mitigate risks and ensure that biometrics remain a tool for security rather than a vulnerability waiting to be exploited.

Before addressing the path forward, it's crucial to understand how we arrived at this point. How did biometrics come into our everyday security uses today? And why has the issue of data protection not always been the centre of our interests? Modern biometrics first gained prominence in the late 19th century, when fingerprinting became a tool for criminal identification. Throughout the 20th century it expanded into civil applications like border control and secure government sites, where it remained a specialised tool for experts. Then, everything changed. The true transformation came with the proliferation of smartphones, turning biometric authentication into an everyday feature. Today, unlocking phones, logging into bank accounts or approving online purchases often requires nothing more than a glance or a touch. In fact, according to Statista, biometrics were the most preferred authentication method in 2023 to sign-in to online accounts, apps and smart devices. The convenience won, without the public asking any questions about data security.

In a world where geopolitical tensions are rising and digital globalisation exposes new security risks, data protection laws like the European GDPR are pushing both governments and companies to rethink their approach to biometric security. Even in a large public sectors as live events, lawmakers from Spain, Australia and South Korea are currently investigating data protection guarantees. Much earlier, in 2021, the French Human Rights Organisation had also appealed to safeguard fundamental rights in the context of specific development of biometric technologies.

As each use of biometrics generates sensitive personal data, we need to think how to protect it at every stage, from collection to storage and beyond.

Cloud computing has revolutionised the scalability of biometric systems, enabling remote authentication and seamless updates across millions of devices. However, this convenience has come with new security risks. Centralised cloud systems have become prime targets for cyber attacks, as they aggregate sensitive data from users around the world. High-profile breaches have demonstrated how vulnerable these systems can be.

According to Deloitte's 2023 Customer Data Privacy and Security survey, 67 percent of consumers are concerned about the misuse of biometric data stored in the cloud. And their fears are right: as reported by IBM in its Cost of a data breach in 2024 Report, 45 percent of all data breaches were cloud-based. This concern is particularly acute in regions governed by strict privacy regulations such as the GDPR. Once compromised, biometric data – unlike passwords – cannot simply be changed. The fear is no longer just theoretical. In 2019, the breach of a major biometric security provider exposed fingerprints and facial recognition data from millions of users, sparking widespread alarm over the long-term consequences.

The healthcare sector is a great example of these risks, as wearable devices routinely collect biometric data like heart rates, oxygen levels and sleep patterns, syncing this information to cloud platforms. If these services are breached, intimate health details could fall into the wrong hands, potentially exposing users to identity theft, insurance fraud or even discriminatory practices.

DEVICES MUST WITHSTAND PHYSICAL TAMPERING AND RESIST SOPHISTICATED CYBER ATTACKS

As global tensions continue to rise, the risks associated with biometric data management also increase. Sensitive sectors like transportation, defence and critical infrastructure depend on airtight security. Unauthorised access can result in severe consequences, from disrupting energy grids to compromising border control. This is especially important as countries like the United States appear to scale back cyber security efforts for political reasons.

Imagine a scenario where the biometric access system of an airport is compromised. Hackers could manipulate passenger data, enabling unauthorised entries, or worse, compromising the entire airport's security framework. Such attacks are not hypothetical – they have already occurred in various forms, prompting governments to reconsider how and where biometric data is stored.

For defense operations, maintaining data sovereignty is fundamental. Military facilities managing biometric records of personnel and secure facilities must guarantee that no foreign entity has access to this information. Sovereign control ensures that national security remains uncompromised, particularly as biometric data increasingly controls access to weapons systems, intelligence archives and sensitive zones.

Localised, or edge, computing offers a strategic response to these challenges and more. Instead of transmitting biometric data to distant servers, it processes and stores information directly on secure devices like smart cards, personal smartphones or local terminals. By reducing data travel, localised systems significantly limit exposure to cyber threats.

For instance, biometric payment cards authenticate transactions via fingerprints stored solely on the card. The verification occurs within the card's secure chip, eliminating the need to share biometric templates with external databases. In airports, some systems now delete biometric data immediately after

a passenger's journey ends, ensuring that sensitive identifiers are not held longer than necessary.

Localised storage not only empowers individuals to maintain ownership over their data, but also aligns with growing demands for privacy and reinforcing principles of data sovereignty. It also reduces dependency on global infrastructure, a significant advantage in times of geopolitical instability.

For industries handling sensitive information and assets – such as pharmaceuticals, energy and defence – biometric security is indispensable. However, the design of these systems must prioritise risk mitigation to avoid creating new points of vulnerability.

INDUSTRIES MUST COLLABORATE TO RETHINK BIOMETRIC SECURITY ON A GLOBAL SCALE

Nuclear power plants now employ multimodal biometric systems, combining fingerprint, iris and facial recognition, to secure critical areas. These layers of authentication ensure that even if one factor is compromised, unauthorised access remains impossible. Military bases have adopted biometric smart cards, embedding encrypted credentials directly on the card itself to avoid any reliance on external servers.

These approaches reflect a growing understanding: securing physical infrastructure requires robust control over digital identities that regulate access. Regulatory frameworks like GDPR reinforce this, demanding strict accountability for the storage and use of personal biometric data.

Still, the protection of sensitive biometric data must be holistic, encompassing all spheres of life and all types of biometric data. For example, a soldier whose biometric data grants access to a national military infrastructure requires high protection of this data not only in the context of his or her work, but also in private life as their fingerprint remains the same. Imagine a scenario where an employee uploads his or her biometric data to a smartphone using a cloud service from a foreign company. This creates potential risks if the data is hacked. If this biometric data is also used to access a strategic infrastructure, the impact could extend beyond personal harm. Some strict legal frameworks could potentially prevent employees from transmitting their biometric data to third-party companies, particularly foreign companies. In parallel, there is an urgent need to raise awareness about the value of biometric data not only for individuals, but also for organisations and, in some context, for national sovereignty.

Localised biometric solutions bring new technical challenges. Devices must withstand physical tampering and resist sophisticated cyber attacks. To meet these requirements, manufacturers are developing tamper-proof hardware and implementing advanced encryption protocols. Biometric templates – mathematical representations of biometric patterns – provide an additional layer of security, making reverse engineering almost impossible. Some countries – and not necessarily the ones you might expect – have already implemented this kind of highly resilient solutions to protect their sovereignty against bigger and more powerful neighboring economies.

But, in all cases, technical solutions alone are not enough. The industry must work together to define best practices, establish international standards and commit to ethical frameworks that prioritise privacy and user control. High-security infrastructures need dedicated regulations to protect them from all risk of hacking biometric data in any context, including employees' private lives. They also need suitable tools to raise awareness among their employees about the issues surrounding biometrics based in public, private or hybrid cloud. In all industries, reducing reliance on centralised systems is crucial to restoring public trust and safeguarding critical infrastructures.

Ultimately, the future of biometric security lies in empowering individuals to control their data. This shift is no longer optional – it is both an ethical imperative and a strategic necessity in an increasingly interconnected and vulnerable digital world ●

Thomas Decker is VP of Product Marketing Finance at Linxens.

Breaches of biometric databases pose a greater threat than traditional credential leaks because the stolen information cannot be modified

Picture credit: Adobestock