Infographics

January 2026

The Security Paradigm Shift of 2026: "Overcoming the Limits of Fragmented Security Management through the Convergence of Physical and Logical Security"

"The Era of Effective Sanctions Begins in 2026" Announcing the Paradigm Shift to Proactive, Preventive Security Systems

About **UNION biometrics**

UNION biometrics is a global leader in biometric security, delivering comprehensive, high-performance access control solutions and premium multi-modal recognition devices built on proprietary technologies and patented anti-spoofing methods, protecting critical infrastructure, corporate, and government facilities worldwide through a trusted global partner network.

Declaring a Paradigm Shift toward Proactive Prevention Security Systems

•The End Point of Insider Threats: UNION Biometrics' Bio-based Physical-Logical Fusion Solution — 'Integrated Authentication Center'

• Accelerating Insider Threats: By 2025, 80% of security breaches will be caused by authorized insiders. Facing a crisis of trust and the limits of traditional perimeter security.

• Strong Legal Liability: Emerging as a management risk that determines corporate survival, including 5x punitive damages and a cap on fines increased to 10% of total revenue.

• Brand Value Bankruptcy: 3.9% of customers churn immediately upon a leak; 80% of potential customers avoid transactions. 40% of business losses stem from the collapse of trust.

• The Technical Solution: UNION Biometrics' bio-based integrated authentication is the most reliable alternative to prevent "Gross Negligence" under the law.

1. Current Status

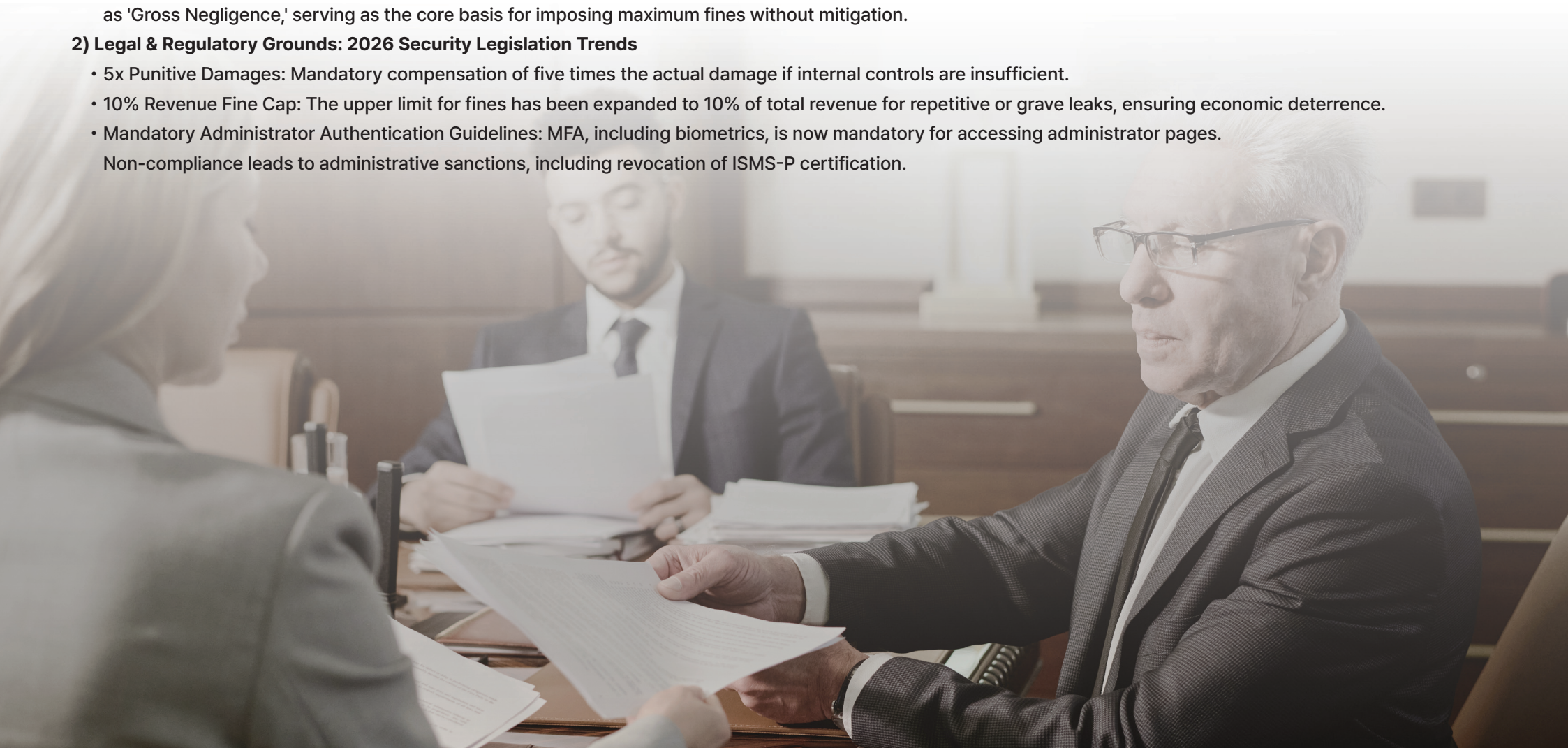
In 2026, the core focus of security is the prevention of personal data breach incidents. Following recent large-scale leaks, the South Korean government and the Personal Information Protection Commission (PIPC) have shifted the focus of security regulations from "post-sanction" to "proactive prevention and technical analysis."

1) 2026 Government Insight: "Legislating CEO Management Liability"

- Under the 2026 business plan, laws are now in effect that hold the CEO ultimately responsible for management oversight in the event of a data breach.
- Incidents involving insider leaks where Multi-Factor Authentication (MFA)—such as non-replicable biometrics—was not implemented are classified as 'Gross Negligence,' serving as the core basis for imposing maximum fines without mitigation.

2) Legal & Regulatory Grounds: 2026 Security Legislation Trends

- 5x Punitive Damages: Mandatory compensation of five times the actual damage if internal controls are insufficient.
- 10% Revenue Fine Cap: The upper limit for fines has been expanded to 10% of total revenue for repetitive or grave leaks, ensuring economic deterrence.
- Mandatory Administrator Authentication Guidelines: MFA, including biometrics, is now mandatory for accessing administrator pages. Non-compliance leads to administrative sanctions, including revocation of ISMS-P certification.



2. 2026 Global Security Priority: 'Broken Trust' by the Numbers

The greatest threat in 2026 is not external hackers, but the "Trusted Insider."

- Astronomical Costs: According to the Ponemon Institute, the average annual cost for global enterprises to handle insider threats reached $16.22 million USD, showing a steady upward trend.
- The Reality in Korea: The majority of technology and information leaks occur due to internal personnel or poor management of internal systems. Corporations must now prove they "did their technical best," or face heavy liability for the entire detection delay period (average 328 days).
- Fatal Collapse of Customer Trust: IBM research shows that business loss due to churn accounts for about 40% of total data breach costs. 3.9% of customers leave immediately, and 80% of potential customers avoid the brand, leading to a market exit crisis.

Economic Impact

Average Global Annual Remediation Cost

$16.22 Million

Approx. 21 Billion KRW

According to Ponemon Institute's analysis, the average annual loss for companies due to insider threats is on a continuous upward curve, posing a direct threat to the sustainability of management.

Detection Gap

Average Detection Delay

328Days

Heavy Legal Liability if "Technical Best Effort" is not proven

The majority of domestic data breaches are committed by insiders. The government is strengthening corporate accountability for the entire duration of the detection delay and demanding "substantial proof of security."

Trust Erosion

Business Loss (Churn) Rate

40%

Risk of Market Exit Beyond Simple Compensation

- 3.9% Immediate customer churn
- 80% Loss of potential customer opportunities

Types of Security Incidents Targeting Insiders

Insider Credential Theft
- Shared/neglected IDs/PWs are the biggest security vulnerability
- Top priority item for 2026 security audit

AI-based Social Engineering Attacks Targeting Insiders
- Sophisticated social engineering attacks impersonating colleagues are surging
- Objective defense with UNION biometrics' anti-spoofing

Insider Path Blind Spots (Physical-Logical Separation)
- Real-time discrepancy between office access and system access
- Need to address the root cause of large-scale internal data leakage

3. The Limits of Online Access Control: "80% of Breaches Start Internally"

Traditional online access controls (Logical Security) like VPNs and ID/Passwords may stop external intrusions but are powerless against authorized insiders.

• **Vulnerability of Credential Theft:** 61% of all data breaches start with stolen or shared 'credentials' (ID/PW). Sharing accounts or neglecting former employees' accounts are top priorities for 2026 security audits.

• **AI Social Engineering Attacks:** Deepfake success rates have spiked. Objective technology like UNION Biometrics' Anti-Spoofing is the only way to defend against sophisticated impersonation of colleagues.

• **Physical-Logical Blind Spots:** 92% of organizations fail to verify in real-time if the person entering the office is the same person accessing the system.

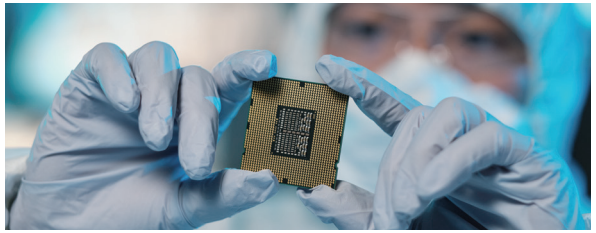
4. High-Risk Sectors:

Where Data Leaks Threaten ContinuitySectorImpact PointRisk Factor

Type 1: Finance & E-Commerce

• Impact Point: Surge in customer churn rate and a bank-run level crisis of confidence.
• Risk: Immediate deterioration of financial soundness upon imposition of fines (10% of total sales). Brand value recovery is impossible in case of insider abuse cases.

Type 2: R&D & Advanced Mfg



• Impact Point: Overseas leakage of core intellectual property (IP) such as semiconductors, secondary batteries, and defense.
• Risk: A single leakage of blueprints/source code by an insider leads directly to the loss of market competitive advantage and a crisis of corporate survival. Expands beyond punitive damages to national security issues.

Type 3: Public & Infrastructure

• Impact Point: Paralysis of national administrative data and power/communication/traffic control networks.
• Risk: Decline in government reliability and occurrence of pan-national liability for damages in case of chaos due to negligence in insider management.

Type 4: Healthcare & Bio

• Impact Point: Leakage of patients' disease information, genetic information, and new drug development clinical data.
• Risk: Due to the nature of the data, it is ultra-sensitive information for which 'original recovery' is absolutely impossible, making class-action lawsuits by victims and years of legal disputes inevitable upon leakage.

5. The Surest Solution: Bio-based Physical-Logical Fusion

1) Establishment of a Biometric-Based Centralized Control Environment for All IT Assets: UBio-Connect

- UBio-Connect ezPass (Terminal Security & Log Management):
  - Face Recognition-Based Login: Implements 'always verification' using dynamic biometric information verified by anti-spoofing (PAD). All history is saved with images to ensure powerful audit trails.
  - Blocking Multiple Logins & Preventing Account Sharing: Blocks simultaneous terminal access and fundamentally prevents unauthorized personnel from using terminals. Realizes the principle of least privilege.
  - Convergence of Physical & Logical Security: Performs cross-verification of the identity (Context-Aware) of the actual person entering the room and the person accessing the system through interworking with the access control system (UBio-X series).
- UBio-Connect PrintGuard (Printed Material Security Management):
  - Integrally manages all OA devices in the company based on the server. Only biometric-authenticated users are allowed to print.
  - Perfectly controls offline leakage paths through detailed logging of printed documents and users.

2) UNION biometrics' Unique Technology: Anti-Spoofing

- Verification by Accredited Testing Agencies:
  - TTA (Telecommunications Technology Association): Conducted Verification & Validation tests on the UBio-X Face Pro v1.0 solution (2025.04.14-04.22).
  - KTL (Korea Testing Laboratory): Acquired K-Mark conformity according to the KTL C 750-2025 standard (2025.06.25-07.15, Report No. 25-035884-02-1). *An access control system capable of distinguishing fake faces.
- Large-Scale Verification Test: Applied anti-spoofing face recognition defense performance test scenarios A, B, and C at face recognition standard distances (80cm, 100cm, 120cm), and performed a large-scale repetition test totaling 17,500 times using various 2D and 3D fake face samples. It passed all test items, proving its excellent fake face defense performance.
- AI-Based Adaptive Update Mechanism: Securing Long-Term Reliability
  - Faces change due to aging, expressions, etc., causing long-term accuracy decline problems. UNION biometrics has secured a patent for an 'AI-based face information update method and device' (acquired in August 2025) to solve this problem.
  - This technology continuously learns the trend of changes in the user's matching score through AI, automatically calculating the most efficient update time and renewing the registration information. Through this, it secures not only immediate intrusion defense capability (Liveness Assurance) but also operational continuity for decades (Long-term Authentication Accuracy) at the same time.

The Surest Solution: Bio-based Physical-Logical Fusion

UNION Biometrics eliminates security gaps through an 'Integrated Authentication Center' that binds logical online security and physical offline security.

- 0.0001% Accuracy: Algorithms lower the False Acceptance Rate (FAR) below 0.0001%, making ID/PW theft or account sharing impossible.
- Innovation in Speed: Real-time authentication in less than 0.2s to 0.5s maintains productivity while meeting government requirements for proactive protection.
- Visualized Control: Secure 100% visibility with access logs that include real-time face images, providing clear evidence for government audits.

3) Core Hardware Systems

- **Fingerprint:** UBio-X LiveGuard – Uses AI-based heart signal analysis (ECG/PPG) for Liveness Detection.
- **Face:** UBio-X Face – 99.9% accuracy even with masks; identifies up to 50,000 users in real-time.
- **Iris:** UBio-X Iris – Provides near-zero error rates for ultra-high security zones.

6. Conclusion: "Enhanced Laws Make Security a Matter of CEO Survival"

In 2026, security is no longer an option but an essential survival strategy. The currently enforced punitive damages (5x) and the upcoming increase in the fine cap (10%) scheduled for 2026 serve as a severe warning to businesses, posing a bankruptcy-level risk to companies with stagnant technical security.

Establishing UNION biometrics' 'Integrated Authentication Center' is the sole practical solution that eliminates the Achilles' heel of insider threats and protects enterprises from stringent government regulations.

7. Self-Diagnosis: Corporate Security Risk Checklist

The more items checked, the higher your exposure to legal/financial risk in

	Checklist	Check
Authenti -cation	1. Does your PC/Laptop login rely solely on ID/PW?	☐
	2. Is MFA (including biometrics) missing for administrator accounts?	☐
	3. Is account sharing common for the sake of convenience?Control	☐
Control	4. Are you unable to verify if the person in the office matches the system user?	☐
	5. Do external/contract workers have high-level access rights?	☐
	6. Are sensitive documents printed without biometric verification of the user?	☐
Opera -tional	7. Would a 10% revenue fine threaten your business continuity?	☐
	8. Would 5x punitive damages cause a fatal blow to your reputation?	☐
	9. Could you survive if a massive number of customers churned immediately?	☐

Diagnosis Results

• 0-3 Items: Basic defense exists, but vulnerable to insiders. UBio-Connect ezPass recommended.
• 4-6 Items: High-risk group. Legal defense for "Gross Negligence" is difficult. Urgent need for an Integrated Authentication Center.
• 7+ Items: An anticipated disaster. Immediate paradigm shift and full adoption of UNION Biometrics solutions required.

References & Legal Grounds

• Legal Basis: [Personal Information Protection Act of the Republic of Korea (Korea Law Information Center)] - Based on Article 39 and Article 64-2.
• Increased Penalty Surcharges: [News regarding the National Assembly passing a bill for fines up to 10% of revenue for personal information leaks] - Example from the latest amendment in December 2025.
• Government Policy: [2026 Major Work Plan of the Personal Information Protection Commission (Policy Briefing)] - Policy plan to legislate CEO management obligations.
• Technical Verification: [Confirmation of UNION biometrics' KISA Anti-spoofing Performance Grade 1 Certification] - KISA Biometric System Performance Test Results.

Data Metric Check (Basis for Calculation)

• Insider Leaks 80%: Based on National Center for Industrial Security Excellence (NCISE) statistics.
• Remediation Cost $16.22 Million: Based on the Ponemon Institute Insider Threat Report.
• Immediate Customer Churn Rate (3.9%) & Churn Loss (40%): Based on the IBM Cost of a Data Breach Report.
• 80% of Customers Avoid Transactions: Based on Varonis and PwC brand trust research results.
• Credential Theft 61%: Based on the Verizon DBIR Report. • Deepfake Attacks 3,000% Increase: Based on the Sumsub Identity Fraud Report.

UNION biometrics Co., Ltd.
Sales Inquiry: +82.2.6488.3207 | www.unionbiometrics.com/en/ | salesinquiry@unionbiometrics.com