Executive Summary:

This project examines cyber breaches in South Korea's financial sector between 2020 and 2025 using open-source intelligence (OSINT) methods. It focuses on trends, common attack methods, and national response measures.

Hypothesis:

Since 2020, the South Korean financial sector has experienced sophisticated cyber threats, with national responses becoming more proactive with prevention, detection and mitigation.

Scope and objectives:

Scope:

Timeframe: 2020-2025
Focus: Banks, fintech companies, payment platforms.
Data: Publicly reported incidents, FSC guidance, government advisories, news reports.

Objectives:

1. Identify trends in cyber incidents against the financial sector.
2. Analyse common attack methods and threat actors.
3. Illustrate findings through case examples
4. Highlight gaps in cybersecurity measures and provide recommendations for the future within the financial sector.

Methodology:

Approach: OSINT-based

1. Data Collection
    - Gather incident reports from FSC, financial authorities, press releases and news sources.
2. Source evaluation
    - Assess reliability and relevance
3. Data Analysis
    - Categorise incident types.
    - Identify patterns over time.
4. Illustrative Case Studies

    - Select 1-2 incidents.
    - Analyse how responses have changed over time.
5. Limitations
    - Only uses open-source based methods.
    - Limited to publicly available information.

Data Collection Log:

Task	Source	Date	URL	Key Info	Tag	Rating
FSC issues cybersecurity advisory outlining suggested policy changes.	Financial Services Commission	2024-02	https://www.fsc.go.kr/eng/pr010101/81638	FSC issued a press release about plans to improve cyber and information security resilience. It describes key strategies of the proposal to provide financial companies greater autonomy and responsibility for managing cyber and information security.	Advisory, Policy Guidance	High
Lotte Card issued an apology for the data breach.	The Korea Times	2025-09	https://www.koreatimes.co.kr/business/banking-finance/20250918/lotte-card-apologizes-for-data-breach-affecting-nearly-3-mil-customers?utm_source=chatgpt.com	Lotte Card issued an apology regarding the data breach that involved nearly 3 million customers. It describes some measures the company will take to prevent future security breaches.	Data breach, Incident response, Malware	High
Shinhan Card reports a data breach affecting merchant records.	The Korea Times	2025-12	https://www.koreatimes.co.kr/business/banking-finance/20251223/s	Shinhan Card reported a breach exposing over 190,000 merchant records. The breach did not affect personal customer data.	Data Breach, Financial Sector, Employee error	High

			hinhan-card-reports-data-breach-involving-190000-merchant-records			
FSC issues press release regarding more recent cyber breaches targeting the financial sector.	Financial Services Commission	2025-09	https://www.fsc.go.kr/eng/pr010101/85367	FSC issued a press release about further plans to improve alertness and response capabilities of the organisations in the financial sector.	Advisory, Policy Guidance	High
Analyze the Lotte Card data breach incident for trends in the South Korean financial sector.	ANDOPEN	2025-09	https://andopen.co.kr/the-lotte-card-data-breach-a-wake-up-call-for-korean-cybersecurity/	Lotte Card experienced a major data breach affecting personal customer information. The incident exposed long-standing vulnerabilities in cyber security measures. Illustrates varying preventative responses needed within the financial sector.	Data Breach, Incident Response	High
Highlight the increasing number of bank accounts being frozen in relation to voice phishing.	The Korea Times	2025-09	https://www.koreatimes.co.kr/economy/20250911/voice-phishing-linked-frozen-bank-accounts-set-to-hit-record-high-this-year	The top 6 lenders in Korea have a large number of accounts frozen after fraud-related (phishing) incidents occurred. Illustrates steady increase in bank accounts frozen since 2020.	Phishing, Incident Response	High

Analysis:

Since 2020, South Korea's cyber threat reporting within the financial sector suggests increased activity by actors, particularly through phishing based attacks. Public reporting suggests that these incident types are steadily increasing, targeting the private sector. These attacks are becoming more sophisticated with voice phishing frequently targeting customers at banks, suggesting persistent targeting rather than isolated incidents.

Several reported incidents have revealed long-term cybersecurity weaknesses, including insufficient monitoring, delayed reporting, and slow response time. These gaps increase the risk of data breaches and prolonged exposure.

National guidance emphasises preventative controls and early detection measures rather than post-incident responses. This reflects the broader change toward preventative risk management within the financial sector.

Public disclosure of incidents has also placed pressure on financial institutions to meet minimum standards set out by regulatory authorities.

The Lotte Card breach demonstrates how long-term vulnerabilities can go undetected over time. Public reporting suggests that insufficient monitoring and preventative measures contributed to the incident, highlighting systemic risks within the sector.

Overall, the financial sector shows gradual movement towards preventative risk management, with increased emphasis on monitoring, threat detection and data protection methods such as encryption.

This analysis relies solely on open-source reporting, which has limitations regarding access to response timelines and measures effectiveness when implemented.

Findings & Discussion:

1. Cyber threats targeting South Korea's financial sector have increased since 2020, with phishing and voice phishing emerging as common attack methods.

2. Several incidents reveal long-standing cybersecurity weaknesses, including insufficient monitoring and delayed detection.

3. National guidance increasingly prioritises preventative controls and early detection over post-incident response.

4. Regulatory oversight and public disclosure pressure financial institutions to meet minimum cybersecurity standards.

5. The Lotte Card data breach illustrates how persistent vulnerabilities can remain undetected without continuous monitoring.

Conclusion:

In summary, open-source reporting suggests that South Korea's financial sector has faced increasingly sophisticated cyber threats since 2020, particularly through phishing based campaigns. Regulatory responses illustrate a shift towards preventative measures, with emphasis on monitoring, threat detection and compliance with policies set by regulatory bodies. Case examples such as the Lotte Card breach highlight how long-term vulnerabilities can persist without preventative controls. While this analysis relies solely on publicly available information, the findings indicate that South Korea's financial cybersecurity posture is gradually moving toward a more preventative and risk-focused approach.